整体攻防训练营

lyouport共创组

战士不应依赖运气，而应依靠准备。—— 山本常朝



整体攻防训练营

1. 序
    1. 云舞白的新生：iyp·整体攻防总述：我们是谁、为何而来… 20年战略图谱
    2. 关于本书
    3. 整体攻防训练营- *iYouPort - Initiatives & Tactics* < *Phase II*> [V1.3.0.20260427]
2. 总教材-CompleteTutorial
    1. S01整体安全 - 总章节：前线安防入门课
    2. 头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
    3. “抓特务” 不是解决方案：整体安全S01E02- 威胁响应
    4. 知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者
    5. 夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产
    6. 每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局
    7. 草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性
    8. 充分的准备和应急反应同样重要：整体安全S01E07 - 计划是 “活的”
    9. 安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动
    10. 您需要真正的 “自己人”：整体安全S01E09 - 进入战斗状态
    11. 协调性很重要，从场内到场外：整体安全 S01E10 - 安全是保持战斗力的绝对必要条件
    12. 抗议中谨防常见危险：整体安全 S01E11 - 协作和互助就是战斗力
    13. 场内协作和场外接应同样重要：整体安全S01E12 - 紧急撤离和汇报评估

14. S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
15. 来自人身的威胁：如何在敌对环境中保护自己 S02E01
16. 最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己S02E02
17. 手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03
18. 为最坏的情况做准备，迎接最好的结果如何在敌对环境中保护自己S02E04
19. S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
20. 在不自由中创造自己的自由：变得难以被追踪的简单方法 S03E01
21. 构建防御直觉是生存的基本功：变得难以被追踪的简单方法 S03E02
22. 与S先生共度美好一天-变得难以被追踪的简单方法 S03E03：反取证技巧
23. 保持零信任 - 变得难以被追踪的简单方法 S03E04
24. 少即是多：变得难以被追踪的简单方法 S03E05
25. 大保健应该成为习惯：变得难以被追踪的简单方法 S03E06
26. 在雷达下低飞：变得难以被追踪的简单方法 S03E07
27. 到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08
28. 8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09

3. 训练-SelfDirectedTraining

1. S01E01-T2 识别威胁并作出反应
2. S01E01-T2 识别威胁并作出反应
3. S01E01-T3 创伤经历如何影响您的认知
4. S01E01-T1 反思现有的安全实践
5. S01E01-T1 反思现有的安全实践
6. S01E01-T3 创伤经历如何影响您的认知
7. S01E02-T2 练习非暴力沟通和反馈
8. S01E02-T2 练习非暴力沟通和反馈
9. S01E02-T1 团队会议安全议题模版
10. S01E02-T1 团队会议安全议题模版
11. S01E03-T1 周围是谁？可视化人际关系图谱

12. S01E03-T2 绘制行为者关系图谱
13. S01E03-T1 周围是谁？可视化人际关系图谱
14. S01E03-T2 绘制人际关系图谱
15. S01E04-T1 清点您最重要的信息资产
16. S01E04-T1 清点您最重要的信息资产
17. S01E05-T3 确认可能遭受的所有威胁
18. S01E05-T2监测自己的压力水平
19. S01E05-T1 制定检查清单
20. S01E05-T1 制定检查清单
21. S01E05-T4 态势监测和威胁清单
22. S01E05-T2监测自己的压力水平
23. S01E05-T3 确认可能遭受的所有威胁
24. S01E05-T4 态势监测和威胁清单
25. S01E06-T1 剖析每一种威胁
26. S01E06-T2 找到弱点建设新的防御能力
27. S01E06-T3 审核防御能力
28. S01E06-T3 审核防御能力
29. S01E08-T1 大家怎么看
30. S01E06-T1 剖析每一种威胁
31. S01E06-T2 找到弱点建设新的防御能力
32. S01E08-T1 大家怎么看
33. 组办安全议题研讨会 S00-T1：为自己定义安全

4. 反渗透/线人&减轻背叛的损失-AntiInfiltration&informant

1. 安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
2. 反渗透/线人&减轻背叛的损失 - 总章节：止损于未病
3. 关于渗透 …… 一些基本须知
4. 什么是“秘密行动”？政府间谍会怎么折腾你…
5. 针对反抗运动的政治渗透：政府线人如何操作
6. 秘密与谎言
7. 了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？
8. 不放弃，不出卖：关于酷刑和证词
9. “我的”朋友还是“我们”的朋友？：如何执行担保措施
10. S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛
11. 您是如何被困住的：审讯心理学 S07E01
12. 巧妙的威胁：审讯心理学 S07E02
13. 无政府主义者生存指南: 了解盖世太保猪式审讯心理游戏

-审讯心理学 S07E03
14. 如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04
15. 在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学S07E05
16. 别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01
17. 为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力
18. 卧底警察识别手册2025版
19. 宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切
20. 中国跨境数字镇压的工业化和私营承包商演变：公民实验室最新报告“Tall Tales”

5. 心理安全-PsychologicalSecurity

1. 安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
2. 不放弃，不出卖：关于酷刑和证词
3. S04完美隐身-总章节：机智是重要实力
4. 直面你的对手 - 6大原则：完美隐身S04E01
5. 了解追踪者的手段和你的弱点：完美隐身 S04E02
6. 思考方式是战略性的：完美隐身 S04E03
7. 技术增值部分 - 最简单的分身方法：完美隐身 S04E04
8. 清扫和清点 - 信息篡改的重要步骤：完美隐身 S04E05
9. 令人兴奋的心理过招：完美隐身 S04E06
10. 用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A
11. 大清洗 - 扫荡危险区域：完美隐身 S04E07
12. 如何欺骗，和如何防骗：反侦基础课 S06E07
13. S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛
14. 您是如何被困住的：审讯心理学 S07E01
15. 巧妙的威胁：审讯心理学 S07E02
16. 无政府主义者生存指南: 了解盖世太保猪式审讯心理游戏-审讯心理学 S07E03
17. 如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04
18. 在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学S07E05

19. S08精神心理安全-总章节：唤回心灵
20. 心理健康训练手册：心理安全S08E01
21. 互助、创伤和复原力：心理安全S08E02
22. 应对创伤：心理安全S08E03
23. 走出绝望：心理安全S08E04
24. 掌控焦虑的策略：心理安全S08E05
25. 运动创伤的处理和应对技巧：心理安全S08E06
26. “没有未来”的未来：沮丧，左派和心理健康的政治 - 心理安全S08E07
27. “你若盛开蝴蝶自来”、“谁痛苦谁改变”、“接受你永远不会被爱的事实”… 自助文化的愚蠢流行及其威权主义本质- 心理安全S08E08
28. 当“反贼”变得越来越像他们的对手… ：打破僵化的激进主义令人窒息的气氛
29. 我们都很焦虑
30. 心里有数：如果您已成为目标：来自内部和外部的威胁和抵御
31. 如何让一个人心甘情愿吐露重要信息？ —— 社交工程攻击“诱导的艺术”
32. 语言是强大的武器 - 如何使用它？人性黑客：致命的诱导
33. 什么是伪装，如何伪装，如何识破 —— 社交工程攻防基础
34. 套话：5种有效的社交工程启发术
35. 夺回你的思想：宣言
36. 宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切
37. (无标题)

6. 组织、照护和互助 - Organizing&SelfCare&MutualAid

1. 设备好像被黑了怎么办？ - 数字急救包
2. S12我盟-总章节
3. 直接行动的组织形成-黑群及其他：我盟S12E01
4. 亲密、身份认同和策略：我盟S12E02
5. 工作中遇到问题。你认为管理层不公平。该从哪里入手？ - 我盟S12E03
6. 开始组织-基础知识手册：我盟S12E04
7. “一对一”的艺术：我盟S12E05
8. 每朵玫瑰都有刺-我盟S12E0N
9. 启动一个无等级的直接行动小组指南：我盟S12E06

10. 如何组织会议：我盟S12E0N+1
11. S13互助生存-总章节：共生的自由状态
12. 如何进行游击分享：互助就是如此简单S13E01
13. 团结而非施舍：互助生存S13E02
14. 构建互助项目：互助生存S13E03
15. 香港生存危机中的反叛政治：互助生存S13E04
16. 从组织到行动：极简战术手册
17. 夺回你的思想：宣言

7. 人际安全&关系结构革命-RelationshipsRevolution

1. 是什么导致队友间不分享知识？
2. 建立国际团结：全球斗争中的人际关系
3. S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
4. 是否有比米兔更好的解决方案？如何？：超越米兔S09E01
5. 恢复团结：超越米兔S09E02
6. 直击性骚扰和性侵犯的根本：超越米兔S09E03
7. 为我们自己负责 - 打破反贼圈子中关于攻击和虐待的僵局：超越米兔S09E04
8. 搬弄权力 - 性癖好与虐待的本质区别 ：超越米兔S09E04
9. 社群集体如何帮助私人亲密关系中出现的问题？：超越米兔S09E05
10. “我的”朋友还是“我们”的朋友？：如何执行担保措施
11. S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
12. 性、婚恋、密友…“反贼”如何构建亲密关系：战友爱侣S10E01
13. 杀猪盘和可利用的同理心：战友爱侣S10E02
14. 亲密关系中的权威主义：战友爱侣S10E03
15. 所谓的“开放关系”可能并不是你想的那种…：战友爱侣S10E04
16. 关系无政府状态的伦理学：战友爱侣S10E05
17. 无界，无级，无限，无尽 …… 无忧，自带安全感的亲密关系：战友爱侣S10E0N-1
18. 构建没有内耗的爱：把我们的亲密关系从资本主义逻辑的泥潭里拯救出来 - 战友爱侣S10E0N
19. S11关系结构革命-总章节
20. 别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

21. 社区应该是什么，是谁在玩坏这个概念：关系结构革命 S11E02
22. 解放结构：关系结构革命 S11E03
23. 如何与内部冲突共存
24. 如何组织社交空间
25. 结识新认识的人时您应该曝光自己多少信息？- 原则和技巧
26. 在这个操蛋的世界里，奋力地相爱！——— 情人节2026
27. 在激进左翼亚文化中恢复团结：关系结构革命 S11E0N +1
28. 创意干预工具包：制止人际暴力实用指南 - 关系结构革命 S11E0N
29. (无标题)
30. (无标题)
31. (无标题)
32. (无标题)

8. 操作安全性 - Digital Security

1. 使用Tor保护自己时千万不要做这9件事
2. 设备好像被黑了怎么办？ - 数字急救包
3. 如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？
4. 使用社交媒体时你必须注意什么？ —— 更安全的抵抗
5. 袜子木偶 - 分身创建的小技巧
6. 移除你的绵羊墙：给普通人的5个防御课程
7. 简易分身术：妥善管理您的在线身份并获得安全的方法
8. 自我人肉
9. 如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？
10. 如何不暴露手机号、不花钱，实现双因素身份验证？
11. 如何保持 Android 设备免受警察的侵害
12. 攻击加密系统的多种形式和防御方法
13. 这些使用暗网的人是如何被抓到的？: 总结教训
14. 如何知道有人正在线人肉你？6个简单的方法
15. 如何检查您的VPN连接是否实际加密
16. 攻击者如何收集有关目标的情报？他们能了解你多少？
17. 如何识别手机上的恶意软件？
18. 在线组织和互助需要多方面小心以维护所有参与者的安全：基本注意事项

19. 您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式
20. 为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式
21. 在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作
22. 给活动家的反人肉指南
23. 泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？
24. 如何才能安全地使用端对端加密（比如Signal）：准则
25. 什么是凭据填充攻击？如何选择密码管理器？
26. 社交媒体上的行动主义安全性:框架手册
27. 他们如何抓捕说真话的人？灾难和教训
28. 某个VPN可能不可靠的5个标志：如果您不理解技术的话
29. 如果您的手机被盗或被警察抢走…
30. 如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击
31. 如何检查MacOS上的恶意软件和键盘监听程序
32. 如何跨社交媒体平台追踪目标人：对抗性思考方式
33. 一次性手机用户指南：关于刻录机电话您应该知道的重要原则
34. 一句话安全须知：记住这些句子，以简单地优化您的安全性
35. Telegram的隐私保护指南，和信息搜索工具
36. 当您准备像编程随想那样工作…：须知
37. 技术是愚蠢的 - 这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

9. 行动安全性-OPSEC

1. 行动安全性总述
2. 在线组织和互助需要多方面小心以维护所有参与者的安全：基本注意事项
3. 在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作
4. 一次性手机用户指南：关于刻录机电话您应该知道的重要原则
5. 安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
6. 直接行动分步指南：它是什么、它有什么用、如何获得成功

7. S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
8. 认识警棍，危害能力和防御方法：街头实战指南 S05E01
9. 头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02
10. 抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03
11. 如何处理枪伤：街头实战指南 S05E04
12. 从雨伞到激光、气球到电动工具：街头实战指南 S05E05 - 战术器具综述
13. 警用武器常见伤害及基本处理方法：街头实战指南 S05E06
14. 充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07
15. 了解防弹衣：街头实战指南 S05E08
16. 您需要真正的自己人 - 如何组成一个亲密团队：街头实战指南 S05E09
17. 了解防暴弹药，以及如何保护自己 ：示威参与者指南 S05E10
18. 让监视摄像头失明：示威参与者指南S05E11
19. 在街上保持安全：街头实战指南 S05E12
20. 和媒体说话时如何避免陷阱：街头实战指南 S05E13
21. 加固横幅和盾牌的制作和使用方法：示威参与者指南 S05E14
22. 占领街头：封锁和阻断指南 -街头实战指南 S05E15
23. 如何启动黑群 - 从准备到行动：街头实战指南 S05E16
24. 反击, 保持自由：街头实战指南 S05E17
25. S04完美隐身-总章节：机智是重要实力
26. 直面你的对手 - 6大原则：完美隐身S04E01
27. 了解追踪者的手段和你的弱点：完美隐身 S04E02
28. 思考方式是战略性的：完美隐身 S04E03
29. 技术增值部分 - 最简单的分身方法：完美隐身 S04E04
30. 清扫和清点 - 信息篡改的重要步骤：完美隐身 S04E05
31. 令人兴奋的心理过招：完美隐身 S04E06
32. 用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A
33. 大清洗 - 扫荡危险区域：完美隐身 S04E07
34. 街头搏击基本技巧（转帖）
35. S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
36. 抢先采取行动 - 反侦基础课 S06E01：七点规则和态势感

知
37. 准确的情报和判断 - 反侦基础课 S06E02: 确立基准线
38. 您必备的基本防身装备：反侦基础课 S06E03
39. 如何摆脱手铐、绳索、束线带和布基胶带：反侦基础课 S06E04
40. 如何撬锁、翻栅栏、短路点火发动汽车：反侦基础课 S06E05
41. 在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C
42. 特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06
43. 警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A
44. 如何欺骗，和如何防骗：反侦基础课 S06E07
45. 武器和自我防御的重要策略：反侦基础课 S06E08
46. 如何在大规模枪击案中幸存：反侦基础课 S06E09
47. 如何检测您是否正在受到监视：监视检测和特殊保护行动
48. 暗中监视的迹象
49. 如何安全地留住证据：给真相的记录者一些技术技巧建议
50. 给公民记录者的技巧指南
51. 公民取证技巧：如何留住真相？
52. 当你手握真相：最基本的防护知识
53. 在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学S07E05
54. 什么是伪装，如何伪装，如何识破 — — 社交工程攻防基础
55. 如何识别抗议活动中可见的和不可见的监视
56. 如何躲避无人机 - 监视时代须知
57. 警察如何利用抗议者的手机追踪每个人
58. 您是否正在被 AirTag 跟踪？这里是检查方法
59. 空中监视如何追踪抗议者？
60. 当您准备参加抗议活动：基本指南
61. 5种常用的“击落”无人机的方法
62. 买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事
63. 直接行动的关键在于协作，但协作的能力并非天生
64. 宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切

10. 纸条- Notes

    1. 不是“个人问题”
    2. 你在人际关系处理方面遇到过哪些尬事？贴张便签，我们聊聊
    3. 安全文化和广阔的生活
    4. 本质主义和身份政治问题
    5. 街头政治对抗技巧提示（就是打架）
    6. 解放教育101:如何培育潜在的同道
    7. 精英主义语言的问题 - 与激进派中产阶级活动家一起探讨
    8. 如何选战友
    9. 需要解决方案，而不是恐惧
    10. 技术与权力
    11. 走出部落
    12. 我们需要更诚实地思考如何组织
    13. 警惕镇压者通过诈骗在你的设备上安装间谍软件：来自意大利的教训
    14. 转帖：从艾未未回国，反思互联网的“伪”影响和流量魔咒
    15. 转帖：关于近日再现的街头镇压毒气弹（传闻可能不准）

11. 技术哲学和技术直觉-Intuition&PhilosophyofTech

    1. “智能城市”究竟是个什么鬼
    2. 小心预览
    3. 即使数据是匿名的，您的身份仍然可以被识别
    4. 礼貌的偏执
    5. 构建技术直觉：生存在数字世界必备的本能
    6. 移除你的绵羊墙：给普通人的5个防御课程
    7. 如何使用社交工程来攻击 2FA？
    8. 地主2.0：科技的新食利资本主义
    9. 你家冰箱如何作为呈堂证供？
    10. 数字取证正在泛滥：政府可以从你的手机中提取哪些数据？
    11. 如何从Matrix中醒来
    12. 警察和间谍如何解码你的照片？
    13. 你的手机如何背叛了民主？
    14. 让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证
    15. 警察查手机的东西长什么样？—— 从技术角度看移动设

备取证
16. 间谍机构使用的开源情报监视方法
17. 一些简单的措施以防止您的汽车被骇客控制
18. 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？
19. 互联网作为新的圈地运动
20. 暗中监视的迹象
21. 当科技巨头走向战争…
22. 聊天机器人的设计“初衷”就是为了让你产生妄想：这不是漏洞，而是商业模式
23. 全球噩梦 - 跨国电信生态系统下的隐形枷锁：公民实验室调查“Bad Connection”
24. 中国跨境数字镇压的工业化和私营承包商演变：公民实验室最新报告“Tall Tales”
25. 超越屏幕
26. “不要再拍了！请关闭设备删除影像”
27. 自由软件的问题… 是资本主义

12. 工具-Tools

1. 安全的云操作系统
2. 一系列元数据工具，从自我保护到有效利用
3. 备份工具 Restic
4. 备份工具 Restic
5. 内存清理 - 寻找文件差异
6. 内存清理 - 寻找文件差异
7. 计算机取证
8. 计算机取证
9. 检查智能手机是否感染了病毒
10. 检查智能手机是否感染了病毒
11. 不联网文档归整
12. 不联网文档归整
13. 去除图像上的水印和不可见标记
14. 去除图像上的水印和不可见标记
15. 预防‘黑头套’
16. 预防‘黑头套’
17. 安全通信 GNUnet Messenger
18. 安全通信 GNUnet Messenger
19. 删除照片中的元数据
20. 删除照片中的元数据

21. 手动检查一个网址是否安全
22. 在浏览器中删除元数据
23. 在浏览器中删除元数据
24. 手动检查一个网址是否安全
25. 查找隐藏的摄像头和防入侵：把移动设备变成监测仪
26. 物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪
27. 防止未经授权的设备访问(老东西)
28. 防止未经授权的设备访问(老东西)
29. 生成假的信用卡资料使注册更安全
30. 生成假的信用卡资料使注册更安全
31. 制作自己的二维码
32. 制作自己的二维码
33. 巧妙地隐藏照片和视频
34. 巧妙地隐藏照片和视频
35. 保密工具：找出是谁把您的文件或照片上传到了网络
36. 保密工具：找出是谁把您的文件或照片上传到了网络
37. 在没有VPN的情况下访问被屏蔽的网站
38. 在没有VPN的情况下访问被屏蔽的网站
39. 断网后通信：把智能手机变成“对讲机”
40. 断网后通信：把智能手机变成“对讲机”
41. 彻底卸载
42. 彻底卸载
43. 在线防病毒扫描器
44. 在线防病毒扫描器
45. 假联系人 - 保护手机通讯录
46. 假联系人 - 保护手机通讯录
47. 绕开审查的浏览器
48. 绕开审查的浏览器
49. 恢复被删除的文件
50. 恢复被删除的文件
51. 从照片中获取元数据的工具
52. 从照片中获取元数据的工具
53. 虚拟手机号和马甲邮箱隐藏真实信息
54. 虚拟手机号和马甲邮箱隐藏真实信息
55. 匿名上传文件以在线分享
56. 匿名上传文件以在线分享
57. 快速搭建自己的VPN服务
58. 快速搭建自己的VPN服务
59. 检查一个应用程序是否有恶意代码

60. 检查一个应用程序是否有恶意代码
61. 读取陌生的/不受信任的USB设备
62. 读取陌生的/不受信任的USB设备
63. 安全的保存您想要的链接
64. 安全的保存您想要的链接
65. 简易P2P信使
66. 简易P2P信使
67. 没有审查的多媒体内容管理系统
68. 没有审查的多媒体内容管理系统
69. 免费的macOS清洁软件
70. 免费的macOS清洁软件
71. 检查您的密码是否被泄漏了
72. 检查您的密码是否被泄漏了
73. 对您的电脑上的文件夹进行加密
74. 对您的电脑上的文件夹进行加密
75. 隐私导向的YouTube界面
76. 隐私导向的YouTube界面
77. 方便的隐私套件
78. 方便的隐私套件
79. 在没有数字足迹的情况下发送秘密信息
80. 在没有数字足迹的情况下发送秘密信息
81. 快速检查可疑程序
82. 快速检查可疑程序
83. 加强电子设备防盗水平
84. 加强电子设备防盗水平
85. 在断网的情况下保持联系
86. 在断网的情况下保持联系
87. 如果你被迫解锁手机，应该怎么做
88. 如果您的手机被盗了或被警察抢走了，怎么办
89. 如果你被迫解锁手机，应该怎么做
90. 如果您的手机被盗了或被警察抢走了，怎么办
91. 安卓恶意软件扫描器
92. 安卓恶意软件扫描器
93. 隐藏秘密信息
94. 隐藏秘密信息
95. 快速构建一个假名账户
96. 快速构建一个假名账户
97. 安全地存储文本(消息、登录凭据、密钥、笔记...)
98. 安全地存储文本(消息、登录凭据、密钥、笔记...)
99. 检查一个网站的安全性

100. 检查一个网站的安全性
101. 远程摄像机/对讲机
102. 远程摄像机/对讲机
103. 检查二维码是否安全
104. 检查二维码是否安全
105. 免费Matrix 消息应用
106. 免费Matrix 消息应用
107. 隐藏一个应用程序
108. 隐藏一个应用程序
109. 类似YubiKey的虚拟USB设备
110. 类似YubiKey的虚拟USB设备
111. 安卓系统防火墙
112. 安卓系统防火墙
113. 匿名偏执狂的选择
114. 匿名偏执狂的选择
115. 在断网后保持通信
116. 在断网后保持通信
117. 一系列安全工具
118. 一系列安全工具
119. 临时/一次性电子邮件服务选项
120. 临时/一次性电子邮件服务选项
121. 在安卓上隔离老大哥程序
122. 在安卓上隔离老大哥程序
123. 开源点对点社交网络
124. 开源点对点社交网络
125. Tor上的加密邮件服务
126. Tor上的加密邮件服务
127. 也是隐写
128. 也是隐写
129. 恢复误删除的数据
130. 恢复误删除的数据
131. 插拔传输代理工具
132. 插拔传输代理工具
133. 安全笔记管理
134. 安全笔记管理
135. 加密文件管理
136. 加密文件管理
137. 检查您的代理是否真的起到保护作用
138. 检查您的代理是否真的起到保护作用
139. 一些匿名的电邮选择

140. 一些匿名的电邮选择
141. 调查区块链上的交易
142. 调查区块链上的交易
143. 安全的云中存储
144. 安全的云中存储
145. 将任何网站变成PDF文件
146. 将任何网站变成PDF文件
147. 开源电邮客户端
148. 开源电邮客户端
149. 一系列安全的即时通信软件和服务
150. 一系列安全的即时通信软件和服务
151. 一些较安全的电邮客户端选项
152. 一些较安全的电邮客户端选项
153. 可自托管的匿名pastebin
154. 可自托管的匿名pastebin
155. 私密电话号码
156. 一些可以欺骗智能手机上的地理位置数据的工具
157. 一些可以欺骗智能手机上的地理位置数据的工具
158. 在Android上加密文件
159. 在Android上加密文件
160. 专注于隐私的安卓网络浏览器
161. 专注于隐私的安卓网络浏览器
162. 创建一个加密的相册
163. 创建一个加密的相册
164. P2P信使
165. P2P信使
166. 在手机上隐藏私密文件和应用
167. 在手机上隐藏私密文件和应用
168. GPS工具
169. GPS工具
170. VirusTotal的官方浏览器扩展
171. VirusTotal的官方浏览器扩展
172. 移动网络浏览器绕过互联网审查
173. 移动网络浏览器绕过互联网审查
174. 安全打开陌生的缩短链接
175. 安全打开陌生的缩短链接
176. 用于去中心化网络的自托管轻量级通信工具
177. 用于去中心化网络的自托管轻量级通信工具
178. 设备间安全地同步剪贴板
179. 设备间安全地同步剪贴板

180. 成为自己的邮件服务提供商
181. 成为自己的邮件服务提供商
182. 取证和反取证工具及资源
183. 取证和反取证工具及资源
184. 对URL进行加密和解密
185. 对URL进行加密和解密
186. 安全搜索
187. 安全搜索
188. 提高安卓设备隐私和性能的工具
189. 提高安卓设备隐私和性能的工具
190. 创建个人VPN
191. 创建个人VPN
192. 安全的即时通信工具 Speek
193. 安全的即时通信工具 Speek
194. 在不安全的渠道上安全传输
195. 在不安全的渠道上安全传输
196. 离线安全传输
197. 离线安全传输
198. 一个功能强大的自托管 Internet 存档解决方案
199. 一个功能强大的自托管 Internet 存档解决方案
200. 通用安卓卸载器GUI
201. 通用安卓卸载器GUI
202. 点对点的匿名安全通信
203. 点对点的匿名安全通信
204. 自动检测链接是否安全
205. 自动检测链接是否安全
206. Telegram探索工具
207. Telegram探索工具
208. 一次性加密笔记
209. 一次性加密笔记
210. 将整个网站转换为PDF
211. 将整个网站转换为PDF
212. 安全浏览器
213. 安全浏览器
214. 无限制传输任何大小的文件
215. 无限制传输任何大小的文件
216. 将手机变成电脑麦克风
217. 将手机变成电脑麦克风
218. 保护安卓手机免受警察的抢夺
219. 保护安卓手机免受警察的抢夺

220. Tor工具系列
221. Tor工具系列
222. 访问网站时保护自己的敏感数据
223. 访问网站时保护自己的敏感数据
224. 基于云的多用户 Chrome 浏览器
225. 基于云的多用户 Chrome 浏览器
226. 绕开面部识别
227. 绕开面部识别
228. 一些注重隐私的浏览器扩展
229. 一些注重隐私的浏览器扩展
230. 一些可选的翻译服务
231. 一些可选的翻译服务
232. 隐私自助：流行产品的开源替代品目录
233. 隐私自助：流行产品的开源替代品目录
234. 一系列隐写工具
235. 一系列隐写工具
236. 浏览器中的流媒体工作室
237. 浏览器中的流媒体工作室
238. 安全地存储秘密
239. 安全地存储秘密
240. 为孤军奋战者准备的预警方案
241. 为孤军奋战者准备的预警方案
242. 打破付费墙
243. 打破付费墙
244. 在坏人强行访问您的设备的情况下抹除数据
245. 在坏人强行访问您的设备的情况下抹除数据
246. 免费读书
247. 免费读书
248. 端对端加密笔记
249. 端对端加密笔记
250. 安卓文件管理器
251. 安卓文件管理器
252. 替换掉那些不够安全的插件
253. 替换掉那些不够安全的插件
254. 免费的去中心化社交网络平台
255. 免费的去中心化社交网络平台
256. 开源笔记应用跨平台
257. 开源笔记应用跨平台
258. 本地托管的 PDF操作工具
259. 本地托管的 PDF操作工具

260. 将安卓手机连接到电脑
261. 将安卓手机连接到电脑
262. 一套鼠标和键盘控制多台计算机
263. 一套鼠标和键盘控制多台计算机
264. 洋葱路由功能的安全信息传递系统
265. 洋葱路由功能的安全信息传递系统
266. 把您的所有消息应用整合在一处
267. 把您的所有消息应用整合在一处
268. 检查可疑电子邮件、链接和文件的在线工具
269. 检查可疑电子邮件、链接和文件的在线工具
270. 开源零知识加密文件共享
271. 开源零知识加密文件共享
272. 安卓加密短信
273. 从视频或音频中总结对话
274. 从视频或音频中总结对话
275. 安卓加密短信
276. 在纯文本中隐藏不可见的信息或水印
277. 安全备份工具
278. 安全备份工具
279. 在纯文本中隐藏不可见的信息或水印
280. 视频隐写术
281. 视频隐写术
282. 分析蓝牙环境是否安全
283. 分析蓝牙环境是否安全
284. 广告拦截
285. 广告拦截
286. 通过临时Wi-Fi 在设备间离线传输文件
287. 通过临时Wi-Fi 在设备间离线传输文件
288. 也是隐写：将敏感信息隐藏在图像中
289. 也是隐写：将敏感信息隐藏在图像中
290. 加密和匿名发送文件
291. 加密和匿名发送文件
292. 一次性密码和2FA应用
293. 一次性密码和2FA应用
294. 去除图像中的水印和其他元素
295. 去除图像中的水印和其他元素
296. 对文件中的敏感数据匿名化
297. 对文件中的敏感数据匿名化
298. 安卓加密图库
299. 安卓加密图库

300. 安全共享
301. 安全共享
302. 完全本地化的开源密码保管
303. 完全本地化的开源密码保管
304. 在任何聊天工具中发送算对端加密信息
305. 在任何聊天工具中发送算对端加密信息
306. 自动检查病毒，并替换为安全版本
307. 临时电邮
308. 自动检查病毒，并替换为安全版本
309. 临时电邮
310. 隐私型安卓网页浏览器
311. 隐私型安卓网页浏览器
312. 安全地隐藏和加密文件
313. 安全地隐藏和加密文件
314. 安卓开源短信网关
315. 安卓开源短信网关
316. 开源 2FA 应用
317. 开源 2FA 应用
318. 以更私密简洁的方式浏览 Twitter/X
319. 以更私密简洁的方式浏览 Twitter/X
320. 安全存储和身份验证管理
321. 安全存储和身份验证管理
322. 开源协作式书签管理器
323. 开源协作式书签管理器
324. 更安全的实时视频会议平台
325. 更安全的实时视频会议平台
326. 一些私密安全的文件传输解决方案
327. 一些私密安全的文件传输解决方案
328. 硬件密码管理器
329. 硬件密码管理器
330. 安全消息应用
331. 安全消息应用
332. 检查密码是否泄漏
333. 检查密码是否泄漏
334. 隐私型电邮提供商的列表
335. 隐私型电邮提供商的列表
336. 从明网搜索 Tor
337. 从明网搜索 Tor
338. 开源剪贴板管理器
339. 开源剪贴板管理器

340. 一系列免费的人工智能翻译器
341. 一系列免费的人工智能翻译器
342. 去中心化的社交网络协议
343. 去中心化的社交网络协议
344. 完全Tor
345. 完全Tor
346. 安全存储照片和视频
347. 安全存储照片和视频
348. 去除图像中的水印和其他元素
349. 去除图像中的水印和其他元素
350. 备份和恢复已删除的文件
351. 备份和恢复已删除的文件
352. 伪造手机位置
353. 使用容器隔离应用程序和虚拟机
354. 使用容器隔离应用程序和虚拟机
355. 伪造手机位置
356. 一些工具都可用来恢复已删除的文件
357. 开源跨浏览器管理器
358. 一些工具都可用来恢复已删除的文件
359. 开源跨浏览器管理器
360. 安卓的网状网络解决方案
361. 安卓的网状网络解决方案
362. 开源加密工具
363. 开源加密工具
364. 匿名托管服务
365. 匿名托管服务VPS
366. 轻量级的高效隐写工具
367. 轻量级的高效隐写工具
368. 备份/恢复工具
369. 备份/恢复工具
370. 给Tor网络研究人员的小工具
371. 给Tor网络研究人员的小工具
372. 聊天IMs
373. 安全IMs
374. 安卓文件管理和清理工具
375. 安卓文件管理和清理工具
376. 来自 GitHub 的AI工具目录
377. 来自 GitHub 的AI工具目录
378. 定期清理硬盘
379. 定性清理硬盘

380. 使用临时网络命名空间通过 VPN 运行应用程序
381. 使用临时网络命名空间通过 VPN 运行应用程序
382. 在不同操作系统之间传输文件
383. 在不同操作系统之间传输文件
384. 将操作系统映像写入USB
385. 将操作系统映像写入USB
386. 加密、生成校验和销毁文件
387. 加密、生成校验和销毁文件
388. 安卓下载器：下载音视频文件
389. 安卓下载器：下载音视频文件
390. 适用于多媒体的跨平台搜索引擎和文件资源管理器
391. 适用于多媒体的跨平台搜索引擎和文件资源管理器
392. URL 检查
393. URL 检查
394. 去中心化无服务器的匿名聊天
395. 去中心化无服务器的匿名聊天
396. 命令行隐写工具
397. 命令行隐写工具
398. 交互式高质量网页存档
399. 交互式高质量网页存档
400. 创建和注入浏览器指纹
401. 创建和注入浏览器指纹
402. 免费下载工具
403. 免费下载工具
404. 在本地运行AI
405. 在本地运行AI
406. 在视频中嵌入隐藏水印
407. 在视频中嵌入隐藏水印
408. 匿名 SIM/SMS 服务
409. 匿名 SIM/SMS 服务
410. 将电子书转换为有声读物
411. 将电子书转换为有声读物
412. 隐私设置终极指南
413. 隐私设置终极指南
414. 清除 Windows 11 中所有垃圾
415. 清除 Windows 11 中所有垃圾
416. 去中心化 P2P 聊天应用
417. 去中心化 P2P 聊天应用
418. 看视频学外语
419. 看视频学外语

420. 极简发布平台
421. 极简发布平台
422. 安全的秘密共享
423. 安全的秘密共享
424. Telegram 语音笔记转录和摘要机器人
425. Telegram 语音笔记转录和摘要机器人
426. 云存储文件管理
427. 云存储文件管理
428. 安全文件存储
429. 安全文件存储
430. 带有频道功能的离线P2P安全通信
431. 一些安全存储照片的方法 [Android版]
432. 绕开KYC 的情况下用加密货币交换加密货币的方法
433. 像1984那样通信
434. 离线求救
435. Telegram内容提取工具
436. 自检URL阻止恶意网站
437. 在 Docker 中运行 macOS虚拟机
438. 专为保护您的照片而设计的相机应用
439. 安卓 - 简单易用的隐私管理器
440. 加密的安卓位置共享
441. 安卓隐私浏览器
442. 终端上的 AI Agent
443. 强制加密密钥 USB 存储
444. 实时语音翻译
445. 寻找代码中的漏洞
446. Google Drive 的开源替代产品
447. 适用于移动设备的Tor浏览器精选
448. 把手机变成临时USB记忆棒
449. 高安全度终端私密聊天
450. 私密P2P的团队IM，无需服务器
451. 开源防病毒软件精选
452. 安全的虚拟浏览器
453. AI文档处理工具
454. 适合高风险用户的通信平台
455. 将数字本文转换为手写字体
456. 谷歌 “查找我的设备”的安全开源替代
457. 安全的剪贴板
458. 自托管文件转换
459. 做移动设备取证和数字调查的开源平台

460. 开源、离网、去中心化的网状网络
461. 生存训练
462. 智能眼镜隐私保护
463. 消除对 Google Web 服务依赖的轻量级方法
464. 隐写工具
465. 取证工具：磁盘分析和文件恢复
466. 反检测浏览器
467. 更安全的密码管理解决方案
468. 隐匿点/安全屋周围Wi-Fi入侵检测系统
469. 隐私型浏览器 - 谷歌浏览器替代品
470. 洋葱网站模版
471. 2025最新的洋葱链接目录
472. 与可信赖的朋友安全地共享位置
473. 文件转换器 - 开源、完全本地化不用云，永久免费
474. 戴面具的电邮
475. 点对点文件传输
476. 离线安全存储 - 完全本地无需服务器
477. 网状网络通信，支持LoRa 设备
478. 2025 年 Tor 使用指南
479. 本地密码管理器
480. 从100多个平台下载视频
481. 用手机作为电脑麦克风
482. 跨平台AI翻译
483. 无云自托管文件存储
484. 互助抗镇压
485. 从普通浏览器进入Tor网络
486. 读书和书籍管理，配AI翻译
487. “干净”的浏览器
488. 一个适用于 macOS 的反取证应用
489. 看看自己在警察眼里长啥样：浏览器数据的取证分析工具
490. 找信号：对抗黄貂鱼等监视设备
491. 免 KYC 的交易平台（精选）
492. 基于人工智能的暗网开源情报工具
493. 从数据库中自动生成美观易读的ER图（给本项目二期工程培训基地参考）
494. 翻译视频
495. 清除电脑上的取证痕迹
496. 家庭管理
497. 3D资源库

498. 有人在悄悄监视你吗？
499. 文件上传恶意软件扫描
500. 自托管黑头套紧急响应
501. Veilid 网络上的匿名私密通信工具
502. 监视资本主义之外的元搜索引擎
503. 注重隐私的智能手机
504. 隐私安全型开源家庭服务器
505. 在不安全渠道上尽可能安全地共享秘密
506. 隐私堡垒门罗币 - 服务清单2026：钱包、交易所、匿名SIM卡、主机及其他
507. 离线知识库：应对灾难和突发状况
508. 跨平台社交媒体情报 - 追踪和自检
509. 暗网调查工具：去匿名化
510. 您的专业级私人情报终端已开源
511. 新闻收割机
512. 安全工具箱规整 - 2026版
513. 开源情报工具库2026
514. 离线图像压缩工具
515. 随手存档
516. 安全的文件存储与共享
517. 自托管AI会议助手
518. 反追踪浏览器
519. 噪声生成式混合网络，比Tor更胜一筹
520. 实时查看您的计算机所连接的位置
521. 把你的Telegram变成无限云存储

13. 威胁知识库

1. 威胁知识库-索引页
2. 镇压手段
3. 自卫措施
4. 带有攻击树的威胁库用例示范
5. 抄家
6. 警犬
7. 关系网络图谱
8. 避免自证其罪
9. 大规模数字监控
10. 偷拍
11. 身份验证绕过
12. 数字取证

13. 人肉搜索
14. 跨国维稳
15. 突袭应对措施
16. 开源情报
17. 大规模数字监控
18. 防篡改准备
19. 藏匿点或安全屋
20. 其他可能出卖您的服务商和机构
21. 审讯心理学
22. 身份检查
23. 指纹
24. 分身
25. 隐姓埋名
26. 物理入侵检测
27. 警方档案(网格)
28. 隐蔽监视
29. 笔迹分析
30. 警卫
31. 匿名购买
32. DNA
33. 痕量证据鉴定
34. 视频监控
35. 告密者（线人）
36. DNA最小化方案
37. 渗透者
38. 道路封锁
39. 有针对性的数字监控
40. 身体暴力 (含酷刑)
41. 掩盖写作风格
42. 反攻
43. 面部识别
44. 背景调查
45. 报警系统
46. 窃听
47. 反监视
48. 步态识别
49. 警犬
50. 定位追踪
51. 对证据的偏见性解读
52. 自行车接力

53. 手套
54. 平民告密
55. 增加警力
56. 公开监视
57. 恶意软件
58. 敲门
59. 户外无设备对话
60. 黄貂鱼
61. 镇压应对措施
62. 警方档案(网格)
63. 跨国维稳
64. 恶意女仆和查抄
65. 被捕支援
66. 网络取证
67. 假身份
68. 服务提供商协助调查
69. 匿名着装
70. 警察巡逻
71. 隐蔽性地突袭住所
72. 监控侦测
73. 语言指纹
74. 警察巡逻
75. 大规模监视
76. 警察巡逻
77. 增加警力
78. 物理监控（上岗）
79. 计算机和移动设备取证
80. 大规模监视
81. 周密的行动计划
82. 视频监控
83. 法医取证
84. 数字技术限制和最佳实践
85. 生物特征隐藏
86. 网络映射
87. 敲门
88. 身体暴力(含酷刑)
89. 加密
90. 移动网络运营商
91. 身份检查
92. 信息最小化原则

93. 地形侦查
94. 元数据擦除和避免
95. 纵火
96. 匿名手机
97. 栽赃
98. 隐蔽的监视设备
99. 弹道学
100. 抄家
101. 空中监视
102. 监视器排查
103. 道路封锁
104. 平民告密
105. 刑侦证据洗白

[image]

云舞白的新生：iyp·整体攻防总述：我们是谁、为何而来 … 20年战略图谱

革命者的机遇正在孕育。

众所周知，对追求激进变革的人们来说，成就感极为稀罕，也因此，无比珍贵。曾经无数前辈终其一生都没能亲见到自己渴望的世界，尽管毫无疑问，他们的积累为今天我们的战斗提供了坚实的基础。

而现在，我们这些人将有可能在有生之年享受到解放斗争的成就感。同时，在此之前，我们可能正在面对的是史无前例的艰辛和险境。

总体上，这绝不是坏消息。但它能好到什么程度，取决于我们的眼界和手速。

BACK

此前不久，Pantone公布2026年的代表颜色名为“云舞白”。鉴于Pantone 一直在使用颜色捕捉时代精神和指导性文化，“云舞白”在网络上引起了很大的争议。

但我们认为，白色恰好符合本项目的核心倡议，即：初学者之心的修为。

[image]

这个时代最不缺的就是各路“专家”，不论是吃官俸的还是自诩的，各种“赛道”上挤满了专业人士，似乎每个人都可能随时趾高气扬不容置疑地宣称自己在某一个或多个领域颇有建树。但这个世界并没有因此变得更好，相反，由于过多的自以为是，我们中很多人将大把的宝贵时间浪费在争执上，在固执己见中不断退化。

我们遗落了什么？

其实，真正的学习不在于学会捡东西，而是在于学会“扔东西”——不断地丢弃过时的知识和惯习、不断摒弃所有先入为主的观念，不断地超越过去的自己，始终保有孩童般纯净的好奇心，挣脱捆绑你的那些“理所当然司空见惯”，拥抱任何新的可能性，进入每一种情境都如初见般灵光闪闪。

创造力就会在每一次新的飞升中浮现。

大脑一直都在不断地成长和变化，每个经历都会开通新的神经通路，每个重复的想法都会加强一些连接，削弱另一些连接。你绝对没有卡在任何一个瞬间，而是在持续构建一个不断发展的大脑。你的意识架构永远在建设中，您完全可以充分利用这种韧性和可塑性。

日本哲学家铃木俊隆曾说过：“初学者脑中有很多可能性，专家脑中却很少。”显然如此。当我们忙于用固有认知反驳任何不同意见时，我们就为自己关闭了新可能性的大门。这是一种最普遍的愚笨。

初学者之心是顶级智慧。冲破所有束缚。心与豁清澄。

白色则是这一智慧的实体化呈现。

白色的本质是没有色彩，但就光线而言，白色是所有颜色融为一体的结果——正如禅宗的核心理念“空性”。空性绝非消极虚无，而是清除成规古旧、迎接无限新希望的胸怀。觉者无执。

一如自决的本质：重塑——我们所追求的自决不仅在于终结统治压

迫、拿回自己抉择的权利，更在于，在抉择的过程中塑造自我 。即革新之力。它远大于普遍人权。我们每个人从出生起就被统治系统灌输并不断内化着各种服务于统治稳定的价值观、意义和理想，而反抗，就是要对此进行不间断的重构和新的建构。

赢得革新之力远比任何一场街头斗争都更加艰巨。 因为这意味着需要你不断打破旧的自己，没有一张“功劳簿”可以让你停下来躺在上面吹牛，也没有哪种舒适圈可供流连忘返忘乎所以。前进是至高无上的也是唯一的成就。

也因此，我们视固步自封为根本性的、真正的危险和障碍。

“我反对教条主义的指责。因为，尽管我对自己的目标清晰明确坚定不移，但我总是对自己所知道的事情抱有怀疑。”——埃里科·马拉泰斯塔

这正是白色所表达的意境。它就像一块空置的画布，等待更多更多卓越的艺术家灵动的手笔，挥洒无止境的创意。每一抹都是开端，孕育万千亮点，每一色都如初见，沁透无暇纯净。每一时刻都可能突现惊喜，下一转瞬便可能出乎意料，机警和期待并存，这很可能令保守者迷失方向，但毫无疑问，将为变革者带来精彩纷呈的奇思妙想。

[image]

iYouPort - Initiatives & Tactics ＜Phase II＞ 的主题是整体攻防。

首先，我们没有称其为“安全”，因为安全是一个战略目标，而不是一个固定的状态，并没有一套能适用于所有情况的通行标准；安全是一个不断抗争的动态平衡，其核心战术就是攻防兼备。

其次，我们没有将其描述为“教材”，而是称其为训练营，尽管本站上线后任何有能力的同道都可以随意取用站内任何主题的资料在自己的本地进行培训工作（具体用法将在接下来的文字中详述）。但我们绝

对希望本站资源不要导致古板的教学关系 —— 这不仅仅是践行无治哲学的方式，更有，这可能是行动者社群在战术创新角度有机会获得突破的关键，即：初学者之心。

真正的教育应该是点燃，而不是填满。

安防领域也没有权威。有很多不同的方法可以达成既定的防御目标，并且永远都会有新的方法出现，安防的成败始终取决于我们能否在战略关键点上比敌人更胜一筹，或至少更快一步；所以，师心自用才是最大的风险所在，固步自封是根本层面的威胁，颜色滤镜会干扰评估和决策的准确性，要小心。

[image]

让新生正式成为战略要点：

连间谍机构都知道在调查陷入死胡同时不是去找更多专业的情报分析师，而是相反，寻求业余人士的帮助以打开思路。现在，陷入死胡同的是整个世界，嘲笑统治精英是草台班子并无助于解决问题，因为我们需要的不是“更专业”的技术官僚，而是彻底革新的勇气。

[image]

消消乐游戏会用抖动来提示玩家“下一步”可能的操作位置，但如果你全程都依照提示行动，你并不会获胜，还可能死的很快。

生活中遍地都是这类误导性的提示，尤其是AI聊天机器人时代、尤其是当聊天机器人的训练数据建立在“主流”砖家的嘴巴上时。

独立思考的能力已经被纳入到了生存刚需技能的范畴。初学者之心实乃救赎之策。

[image]

预测局势，及其战术指导意义

我们每年都会通过年终礼预测短期前景和局势。今年我们想要谈论一些更长远的前景，毕竟，21世紀已经结束了四分之一，一个显著的趋势动态也已经开始成形。

显然，我们目前还处于人工智能与人形机器人相结合所带来的生产力飞跃的萌芽阶段。这些机器人能够承担大量无需多少创造性投入的“常规”任务（从照料老人到送货上门，更不用说在流水线上执行简单的机械操作了）。这一转型带来的社会乃至政治后果可能很多难以尽述，但至少以下几点，应该现在就提起注意：

1.

发达国家大量剩余劳动年龄人口的涌入，任何职业再培训项目都无法弥补这一缺口。唯一的解决办法是通过保障收入制度来照顾这部分人口。但这会带来弊端，即导致他们更加贫困。

反抗情绪将飞快增长，任何想要遏制这种反抗情绪的政策和镇压措施都会对代议制形成巨大的挑战。

2.

由于移民流动受阻，富裕国家与贫困国家之间的紧张关系会快速加剧。

富裕社会将大幅减少对临时性的、劳工移民的输入需求，并开始封闭自身的小世界，阻止任何外部势力的渗透。

这将导致某种程度的全球隔离，并催生出“保留地”。人们会不惜一切代价逃离这些保留地，哪怕生命受到威胁。

3.

大众教育将受到质疑。操作机器人只需要相对较少的原始技能，而控制机器人则需要高质量的教育，这显然无法普及。

教育实践和“文化消费”结构的改变将导致相当一部分人口认知能力的下降，进而导致更严重的阶级分化，并滋生新的冲突根源。在这种情况下自由派中产的改良主义模型将难以为继。

[image]

BACK

BACK

由此可见，社会内部和外部的紧张局势都将呈指数级增长。这一状况下，古旧的“公民社会”和“ ”都已经失去能力。换句话说，中产阶级改良主义的方案将在未来几年内快速衰退。这本身就可能产生显著动荡。

如果任何人认为这种情况发生在遥远未来，那就肯定错了。按照目前的技术发展速度，这种情况在十几二十年内就很可能发生，这意味着我们中大部分人都会在有生之年亲见。别忘了，还有同样剧烈的气候变化在此基础上同步发生。

由此，一方面，爆发全球军事冲突的可能性会极速升高；另方面，解放者的倡导力也很可能空前顺畅。后者迹象目前已经初露端倪。

这一局势的指导意义在于，倡议和示范工作中两个场域被突出出来：气候正义和流民自治主义。如果您已经在相关方面有基础，那是极好的，目前还没有也没关系，现在开始完全来得及！

[image]

BACK

是的未知因素非常多，激动的同时也很可能令人忐忑。但我们现在讲

述这一局面并努力去理解它，毫无疑问将能够成为一种凝聚人心的重要理念，引领我们大家走出这个巨大的未知。

[image]

“21世纪的文盲不是那些不会读写的人，而是那些不会学习、忘记和再学习的人。”

——艾尔文·托夫勒，《权力转移：21世纪的知识、财富和权力》

[image] 在我学习到中文新词“邪修”的意思后，我发现这是个很不错的亚文化，带着一种重要的洞察，并因此可能具有广阔的潜力…… [image]

“整体攻防训练营”使用说明

1、导航说明

建议您使用每一套教程之前都从相应系列的“总章节”页面进入。

在主页上部，您将看到两个折叠标题：

1. “整体攻防训练框架” —— 这一部分包含14套教程，适合前线社区的新队友，或者培训工作的组织者。如果您正在准备全面学习，我们推荐按序号推进。

1. “威胁知识库” —— 这是一个实战价值很强的架构，它从威胁和防御两个方面切入，勾画出一个完整的直接行动安全性知识系统。还包括一个示范，以引领您在现实环境中应用这一工具。

[image] [image]

本项目基于**DIY**理念，即注重自主权和可及性，任何合作者都可以基于您的本地需求将教材进行本地化处理，我们相信实战中的前线工作

者最了解自己需求什么。

2、版本说明

进入首页后，您会在标题末尾看到版本号。这是本项目第一次使用版本号标记更新进度。

[image]

目前您正在使用的是1.0版。每一次显著的更新后我们都会同时更新版本号，让跟随一目了然。

1.0 版本并非完整态。因为这项工作是 iYouPort - Initiatives & Tactics 项目共创公社的试运营，编写工作与地方训练营实践项目同步进行，所以，完整上线的部分是已经运行完成的部分，而尚未完成的部分将在年后开工时继续进行，届时将同步更新。

3、关于时间安排

我们和合作方从现在开始休假。和往年一样，将于**2026年3月23日**复工。届时本项目进入2.0版的更新阶段。完成时，您将在首页看到“更新公告”。

中国年后我们将开始在 iyouport.substack.com 的推送。每周两次，每周二和周五两天订阅者将收到更新进度邮件。

如有特别通知，将在周日发送。

4、强调

本站点、和本项目站点网络中的所有站点，均可一键复制到您的私人账户中，并按照您需要的格式导出到本地，供离线使用。

所有参与首轮试运营工作的地方培训师和协助者、以及任何形式的贡献者，请不要公开转发本项目。

并且，尤其建议用户使用Tor网络浏览和制作副本到本地。

请不要使用任何公共打印机印刷本项目内容，以及使用本项目内容进行的任何形式的再创作。

不要 使用AI“提纲”； 不要将 本项目中尚未翻译的文档资料放入AI。

练习。练习非常重要，任何技巧和技术只有通过不断练习才能真正变成您自己的东西，才能在您需要的时候发挥作用。

[image]

Q&A：IYP回复二期工程合作方最感兴趣的问题

1、“共创公社”是什么？为什么从项目二期工程启动，而不是一期理论部分？

是的，本项目（iYouPort - Initiatives & Tactics）整体是一个互助项目，而不仅仅是二期工程 —— 尽管必须说二期工程是目前最突出的互助协作成果。

这份成果来自我们与所有参与共同实践的朋友和前线社区的精心培育。共同的信念和解放斗争的战略共识是我们彼此唯一的纽带。这其中没有任何人具有特殊身份，没有指挥官，没有士兵，我们每个人都对自己的贡献负责，同时也对本项目整体的前进方向负责。

“共创公社” 是一个无等级的网状网络协作实践。在这里，没有任何权威支配他人，没有人能垄断资源，没有交易性和工具性人际，所有合作方从互助自治中获益。

“共创”和“公社”这两个元素对攻防战术领域的成功至关重要，这就是为什么该实践从二期工程启动。

关于“共创” ——

与课本知识不同，对我们这些反抗者来说，能保护我们安全和帮助我们实现变革目标的知识，大多来自于前人的经验教训和各种刻骨铭心的试错历程。每个时代的镇压系统都会致力于清除这些知识，而反抗者则竭力保存它们，并不断更新升级，以适配新的镇压机器。

所以，任何有效的安防技巧和战术策略都将毫无疑问来自无数英勇前辈的实际积累，并同时由无数无名后辈悄悄流传和维护。没有共创精神就不会有反抗领域今天的成就。任何竞争心和私利欲都会损伤其价值，破坏其发展前景。

关于“公社” ——

为延续反抗前线的生命力，滋养我们的知识系统需要一群理解互助自治的政治哲学的人悉心维护，权力均等、资源透明的公社关系结构可帮助大家更好地达成目标。

“共创公社” 没有围墙。有心者可在任何时候复制本项目的工作、对其进行必要的“再”本地化、或者更多您认为恰当的重新组合。

最后强调，这里很多知识都是隐性的，学习者需要在经验中领会并将知识体系补充完整。所以，反馈很重要，“共创公社”依赖实践中收获的反馈来不断更新自身。

不断成长，不断发育，保持初学者之心，将是我们的制胜法宝。

您可以在下面下载“共创公社” 运行模式的简要架构描述PDF：

 将鼠标移动到右上角，选择下载，或“查看原始内容”
attachment:4051fa9e-e4fd-44e8-a1cb-70d20c75e0a1:___共创公社____-_共同创作，相伴成长_-.pdf

在此，**IYP**只是策展人。真正的智慧来自全世界久经沙场的反抗者和无数后勤经验丰富的无名战友。

我们从来没有教您去做任何事，也永远不会这样做。感谢您记得这点。

2、为什么建议“使用Tor浏览器阅读”？

因为本项目中包含比较激进的内容。为了长远发展考虑，我们希望大家习惯于一些基本的安全措施。

必须激进吗？

不是“必须”，准确说应该是“不得不”将激进战术纳入考虑。

老一代异议人士所熟悉的公民抗命、非暴力原则云云，在当前这个暴政横行的时代都不再能起效。因为它们起效的前提是 —— 假定对手会害怕、假定对手无法对大群体造成永久性的伤害 —— 这些基础都没有了，无数事实证明镇压系统致力于不惜一切地捍卫政权，视人命如草芥。即便在万不得已的情况下政权许诺做出妥协，也不过是断尾求生之举，并不代表行动的有效性。

真正的有效性取决于行动项目对统治体系构成的冲击。

冲击力是行动者的智慧、机敏、韧性、创造力和专业知识共同达成的 —— 其基础是人，和人际。

仅仅“大基数”不是制胜法宝。团结一致防御稳固的大基数，才是关键。

正如我们穿上全套护甲以避免被毒气和子弹击倒，同样的，我们必需能保卫自身不能被神经症竞争和渗透告密所侵蚀、不能被社交工程欺诈和审讯心理战的操控俘获、不能在间谍软件的零日灾难中变得虚无绝望，同样不能在焦虑抑郁的沼泽中沉沦。

当您能意识到脆弱性可能发生在任何地方时，您就会理解，“安全”必需是一整套全方位多层面的防护策略。

安全策略的部署和战术部署密切配合，不可切分。同样，讲述安全原理时如同讲述战术原理时一样都可能涉及想象力的牵引，这难以避免。我们希望学习者尽可能发挥框架思维，举一反三，将您和队友的隐性知识经验以恰当的方式结合到本项目的议题中来，一来可实现更贴切的本地化，更有，本项目的大背景即我们与您的共同战略，也将由此赢得不断成长的生命动力。

[image]

“激进”一词源于拉丁语“根”，与其词源相符，当今的激进实践也应采取植物学的视角：培育一个滋养我们的系统，而非一个毁灭我们的系统。

3、透露防御技巧会不会反而帮助’坏人’提高了技能呢？或者会不会提示坏人关于如何绕过防御的办法？

对于第一个问题，答案就是：“坏人”在敌对监控方面通常不需要太多帮助。他们对此早已非常娴熟，相反，那些一无所知的人是他们攻击计划的目标，也就是那些“好人”，因为“好人”几乎没有理由去思考或体验这些东西。

获得技能主要是提高您的防范意识和威胁敏感度，并获得一些经验

—— 是大多数“坏人”已经做过的事。他们还会继续做下去，现在您有必要了解这些事。

至于第二个问题，答案也是否定的。为敌对计划者配备有关保护性操作的一般知识并不能真正帮助他们绕过或逃避安全措施（只要信息不太具体。传授这些知识的人肯定有分寸）。

最后，请始终记得，带着初学者的灵气，不要停留在任何文本的表层，而是视其为踏板，让创新能力带领您飞升。

4、你们将这一项目定位为专门为无政府主义社群服务吗？左派呢？你们是否反左？

绝不是。本项目没有意识形态局限性。我们也不“反左”。相反，我们与左派很接近，但有区别。

无政府主义运动和左派运动的典型区别在于，左派总是需要足够多的支持者，俗称人头，因为他们的战略是用新的权威去取代旧的，统治系统不变。要做到这点就必须“转移”旧权威的支持率，到新权威上。于是他们会花大量的精力去劝导、动员、拉拢人们。

而无政府主义者则不需要。因为我们所期待的是取消整个等级体系，废除统治本身，而不仅仅是个别统治者，把主宰人生的权力交还到每个人自己手中。我们通过两种方法实现这一战略：冲击，和示范。冲击旧的，示范新的。用冲击来示范，用示范来冲击。

我们希望通过我们的努力可以激励人们意识到完整的能力就在自己身上，佛家所言之“本自具足”，只要一个人想要获得解放，TA就可以为自己争取到，无需领袖、无需司令、无需政府和老板。

所以无政府主义运动不需要很多“追随者”，尤其是点赞付费那样的虚伪追随，完全没有意义。无政府主义不是意识形态，它是一种思想，一种相信去除所有等级压迫、追求无限延展的自由和自主的世界是可

能的思想。就如维特根斯坦所言，思想是无法标价的，能“支付”思想的唯一方法，是勇气。

您无需声明自己的是什么主义者。这里真正重要的是行为，而不是装束。多元主义和自由与任何正统意识形态都格格不入。正统意识形态对此的声称都是骗局。

不要粉丝？那这个项目想要达成什么目的呢？

是的不需要寻常的关注。本项目不是要说服任何□相信任何事情，也不是想让任何□成为我们的追随者。我们希望□们独□思考，□他们的批判能□去理解和分析他们周围的世界。

本项目所有内容都是前线社区认为有□的知识点。攻防战术始终在升级，所以没有长久定论。我们始终对颠覆性的思想和实践持开放态度。我们希望找到对这个项□的成长发展感兴趣的更多创新者，□论他们有什么标签。

我们通过建立网络来应对上述时局，因为没有人能够独自战斗或长期独处。这种联系建立在亲近和友谊之上，绝非强迫性的社群，在那种带围墙的社群中，人的理想、愿望、梦想和需求都会被迫屈从于一种诡异的共识。不论该共识当时看起来多“进步”、多“伟大”，围墙结构早晚会让这样的社群变得专制、死板和退化。

5、很多人表达异议只是为了寻求移民庇护。IYP支持移民吗？都移民了就没人反抗了吧？

首先，我们永远支持“移民”。或者准确说，我们通过反对“移民”这个概念来支持迁徙自由 —— 作为人，就如所有动物一样，我们本就应该有权生活在任何一个我们认为适合自己需求和发展的地方；而不是作为“民”，即便迁徙成功也只是意味着换一套臣服对象。

其次，本项目的服务面向不受国界限制，就如本项目的合作方不受国

界限制，攻防技能和智慧来自所有不甘于统治压迫的人类。不论您住在哪里、使用哪种语言，都不影响本项目的战略目标。

不仅如此，任何“身份标签”，都不影响本项目的战略目标。仅仅是…… 对于臣服者来说 —— 不论是原地臣服、还是千山万水远渡重洋的臣服 —— 他们可能很难感受到本项目大部分的重要性和意义。

如前文所述，流民自治和气候正义是未来十几二十年内的重要变革驱力，所以我们的确希望本项目的用户以自由解放的大战略为目标，而不是狭隘的粉黑嘴炮。

6、反贼总是像战斗机一样，看着好累。你们也是这样的吗？

本项目是抵抗区，同时更是疗愈区，尤其本项目的心理安全专题，有详细的教程指导致力于帮助人们从严重的创伤中恢复过来。

要想真正实现变革，我们肯定不能只依赖攻击。事实上反抗者需要更多的休憩、更多爱的抚慰。捍卫福祉是我们最重要的战略方向 —— 自由和平安相辅相成。

7、谁是IYP？

任何人都可以是IYP，也可以不是。如果您受够了当下压抑无聊的生活、不甘心在委屈愤懑中燃尽一生、想要摆脱勾心斗角心机算计的灰暗关系、不想继续在各种无形的胁迫和束缚中痛苦沉淀 …… 尤其是，如果您意识到了改变的紧迫性，您渴望亲手打造未来自主决策，而不是把自己的命运拱手于“下一批”统治精英，那么，您就是“IYP”。

不要寻找组织，要寻找盟友，有了盟友自然就会有组织。

不要寻找IYP。要寻求创新的战术。成为IYP。

[image]

希望本站各栏目的研究主题能够在社会运动内部引起更广泛的讨论，激励各方有志之士更努力地投入资源以探讨如何保护变革运动的可持续性发展。

请记得，在解放斗争中，任何文本都存在局限性 —— 真正珍贵的资源始终都是并肩而战的你我彼此和我们所有人相互扶持的关系结构。

[image]

欢迎开启旅程！□

关于本书

本书内容来自于站点:

https://iyouport.notion.site/iyp-20-28c34ca2d46d80289dfff59511fd7022

随着站点内容的增多，本书可能每半年到一年出一个新版。

阅读建议：

- 在离线的设备或虚拟机上阅读
- 和原版网页比对后再阅读，电子书的排版和网页不完全一致，且不包含视频和pdf
- 多用目录

隐私与安全告知：

意外联网的可能。简单理解epub/mobi/azw文件是包含一系列网页文件的zip压缩包。如果网页文件中有外链的图片，您的阅读软件就会自动联网下载它。虽然本书特地剔除了需联网加载的资源，但不排除有考虑不到的地方。如果您的网络环境不安全，请离线阅读。

功能受限/缺失：

- 网页内嵌的视频、音频、pdf、epub、社交媒体引用在本书中都将无法使用
- 少量图片缺失。随书附上缺失的图片链接。
- 部分阅读软件可能无法正常显示动图。
- 本书是从网页自动转换的，因此可能有少量结构特殊的网页视觉效果不佳。

本书缺少的图片

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

超越屏幕 6681802e3321832c9999815244a9a7e2.html

图片链接:https://www.splingmovies.com/wp-content/uploads/2023/10/beyond-the-screen-4.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

身份验证绕过 6821802e332183e98e0981884d4e9076.html

图片链接:https://www.ncsc.gov.uk/images/library/authentication-methods.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

让监视摄像头失明：示威参与者指南S05E11 1ff1802e33218341936581 38e157c2d3.html

图片链接:https://macleans.ca/_next/image/?url=https%3A%2F%2Fcms.macleans.ca%2Fwp-content%2Fuploads%2F2014%2F09%2FMAC40_HONG_KONG_FEATURE012.jpg&w=640&q=

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

当“反贼”变得越来越像他们的对手…：打破僵化的激进主义令人窒息的气氛 a611802e3321830fa936813468d96df2.html

图片链接:https://z-library.sk/apple-touch-icon.png?v=1

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

构建技术直觉：生存在数字世界必备的本能 5651802e3321833eb59881ca48979584.html

图片链接:https://static.vecteezy.com/system/resources/previews/021/039/772/non_2x/wisdom-education-or-philosophy-knowledge-and-learning-understanding-or-intuition-critical-thinking-or-creativity-study-concept-human-head-with-bright-lightbulb-metaphor-of-wisdom-and-education-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

如何检查MacOS上的恶意软件和键盘监听程序 c641802e3321821688b00181f4771797.html

图片链接:https://static.vecteezy.com/system/resources/previews/007/151/172/non_2x/cyber-security-icon-doodle-hand-drawn-or-outline-icon-style-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

每朵玫瑰都有刺-我盟S12E0N
0ed1802e332183c19ea1013e526058d2.html

图片链接:https://media.istockphoto.com/id/1344634305/vector/people-waiting-in-queue-male-and-female-characters-stand-in-line-look-on-wrist-watch.jpg?s=612x612&w=0&k=20&c=-Sh1BaCGL--gysBKUm-ibGoAInF7bp0mLIrBqhfHk6g=

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

更安全的密码管理解决方案
5d81802e332182d2a1a0814fb780da68.html

图片链接:https://camo.githubusercontent.com/ec8d1ccd6955dd7205779df000248c3d4efaed57322170569754 5ce3252781

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

将数字本文转换为手写字体
23f1802e3321825fa94a81f8ebf34635.html

图片链接:https://github.com/dovbyk/DeepScript/raw/main/frontend/public/output.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

杀猪盘和可利用的同理心：战友爱侣S10E02
e781802e3321834681158 15d6e50be8a.html

图片链接:https://static.vecteezy.com/system/resources/thumbnails/057/976/343/small_2x/young-man-rejecting-loving-woman-male-and-female-characters-experiencing-unrequited-feelings-one-sided-or-rejected-love-flat-illustration-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

袜子木偶 - 分身创建的小技巧
07c1802e3321832cb28f0199ac8d6d88.html

图片链接:https://static.vecteezy.com/system/resources/thumbnails/010/338/451/small/single-continuous-line-drawing-businessman-loves-to-look-at-his-reflection-in-mirror-with-thumbs-up-pose-man-in-mirror-reflection-egoistic-attractive-confidence-one-line-draw-graphic-design-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

从100多个平台下载视频
5441802e33218350adca81ed62a0d70f.html

图片链接:https://vidbee.org/_astro/ui-rss.-gV58W0B_2q4I6j.webp

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

本质主义和身份政治问题
c451802e33218337bbb18155648e4100.html

图片链接:https://static.vecteezy.com/system/resources/previews/057/645/121/non_2x/stickman-holding-a-flower-mental-health-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

您需要真正的自己人 - 如何组成一个亲密团队：街头实战指南 S05E09 a071802e332183f4aea6819601cb1b7f.html

图片链接:https://www-s3-live.kent.edu/s3fs-root/s3fs-public/styles/teaser_image/public/page/cbsn-fusion-former-kent-state-students-speak-out-50-years-after-deadly-protest-thumbnail-478589-640x360.jpg?VersionId＝UTk46m6ycQud80RNitXSTwr1.Bv1g91Q&h＝d1cb525d&itok＝

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

从组织到行动：极简战术手册
6ea1802e3321837aa15f814d1b87b221.html

图片链接:https://www.coe.int/

documents/24832180/27713469/0/54d9a8cc-bad7-24b5-581c-effc9fc1208f

==================================

有针对性的数字监控 44d1802e3321832586c58101bd083cd2.html

图片链接:https://www.amnesty.org/en/wp-content/uploads/2021/06/273025-1444x710.jpg

==================================

结识新认识的人时您应该曝光自己多少信息？- 原则和技巧 8621802e332183109c508139db1122f5.html

图片链接:https://static.vecteezy.com/system/resources/previews/011/141/850/non_2x/couple-in-love-young-family-romantic-relationship-isolated-cartoon-illustration-vector.jpg

==================================

窃听 2f41802e3321833cac6e017617580587.html

图片链接:https://www.cctvcamerapros.com/v/images/audio-surveillance/android-app/remote-audio-surveillance-android-app.jpg

==================================

一次性手机用户指南：关于刻录机电话您应该知道的重要原则 fc01802e3321820e9ab4016df13cf768.html

图片链接:https://static.vecteezy.com/system/resources/previews/071/599/897/non_2x/smartphone-security-shield-line-and-solid-icon-set-mobile-protection-and-data-privacy-symbol-collection-cybersecurity-and-safe-browsing-isolated-illustration-vector.jpg

==================================

对证据的偏见性解读 0d81802e332182e2987181d9bce3e1db.html

图片链接:https://upload.wikimedia.org/wikipedia/commons/thumb/4/4e/Justice-OldSupremeCourtBuilding-Singapore-20071013.jpg/1200px-Justice-OldSupremeCourtBuilding-Singapore-20071013.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

网络取证 8031802e33218356b046814e84ee1c65.html

图片链接:https://encrypted-tbn0.gstatic.com/images?q＝tbn:ANd9GcShnEu2-qINa-tc8KKMKrvfp-X2XXQNWhjcGQ&s

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

反检测浏览器 0af1802e332182f8834f0125eb3c3eb2.html

图片链接:https://camo.githubusercontent.com/7bda7bc1ff299c576004f53c257d4b7a37bf5c1

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

整体攻防训练营- *iYouPort - Initiatives* & *Tactics Phase II* eff1802e3321837faed881f365fda52c.html

图片链接:Monosnap_Image_2025-12-13_00-29-49-removebg-preview.png

本地图片文件名:Monosnap_Image_2025-12-13_00-29-49-removebg-preview.png

图片链接:Monosnap_Image_2025-12-13_00-29-49-removebg-preview.png

本地图片文件名:Monosnap_Image_2025-12-13_00-29-49-removebg-preview.png

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

大规模监视 97e1802e3321838a95140120b71023de.html

图片链接:https://www.ft.com/__origami/service/image/v2/images/raw/http%3A%2F%2Fcom.ft.imagepublish.upp-prod-

eu.s3.amazonaws.com%2F57b28b10-8a77-11e8-bf9e-8771d5404543?source＝next-article&fit＝scale-down&quality＝highest&width＝700&dpr＝1

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

大清洗 - 扫荡危险区域：完美隐身 S04E07 42d1802e332182bca8d3011f3f14679a.html

图片链接:https://familynews.today/wp-content/uploads/2022/07/escape-door.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

大规模监视 1ba1802e3321838db40a81c3ee7cc059.html

图片链接:https://www.ft.com/_origami/service/image/v2/images/raw/http%3A%2F%2Fcom.ft.imagepublish.upp-prod-eu.s3.amazonaws.com%2F57b28b10-8a77-11e8-bf9e-8771d5404543?source＝next-article&fit＝scale-down&quality＝highest&width＝700&dpr＝1

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

反击, 保持自由：街头实战指南 S05E17 22e1802e33218279abf581cf905aed8a.html

图片链接:https://peacerep.org/wp-content/uploads/2023/12/Corruption-is-the-lifeblood-of-politics-in-Iraq.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

与可信赖的朋友安全地共享位置 4b61802e332182078c8881bff79c89cb.html

图片链接:https://camo.githubusercontent.com/238e6bc1be7807d1161911fa4b1ce451ca3a4

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己S02E02 08d1802e332183c3b6f981ffa1a2b42c.html

图片链接:https://www.boldbusiness.com/wp-content/uploads/2022/06/Cyber-Security-Banner.png

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

网络映射 f0f1802e332182d8951901b3c021c76f.html

图片链接:https://resize-v3.pubpub.org/
eyJidWNrZXQiOiJhc3NldHMucHVicHViLm9yZyIsImtleSI6Imxvb243dXRpL

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

创意干预工具包：制止人际暴力实用指南 - 关系结构革命 S11E0N cc51802e332182df952981943205f3dd.html

图片链接:https://static.vecteezy.com/system/resources/thumbnails/013/827/813/small/diversity-group-people-social-equity-and-inclusion-free-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？1a11802e3321824ab98081e81ad464cf.html

图片链接:https://static.vecteezy.com/system/resources/previews/011/012/997/non_2x/single-one-line-drawing-businessman-putting-big-key-into-smartphone-data-privacy-for-protect-internet-user-password-and-login-device-security-system-continuous-line-draw-design-illustration-vector.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

纵火 ebe1802e3321824da36b81a8e87517c4.html

图片链接:https://atslab.com/wp-content/uploads/2024/05/Forensic_Arson_Automobile_Theft_Investigator.jpg

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03 8481802e332183c186c801c9c98cd9d2.html

图片链接:https://www.cisco.com/c/dam/assets/swa/img/anchor-info/cisco-powered-services-628x353.png

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 0c71802e332182c79d628168c3fe6d1c.html

图片链接:https://files.virgool.io/upload/users/1481874/posts/v5pxdzmcptzu/ysirbldfoddp.png

[image]
[image]

整体攻防训练营- iYouPort - Initiatives & Tactics < Phase II> [V1.3.0.20260427]

iYouPort : 本项目并非阅读材料。我们制作的不只是“文章”。
我们正在搭建的是一个平台，用以收纳、展现、调试和更新一系列 方法、工具、战术智慧和装备 ，
并通过这一过程，示范一种新的关系结构 —— 与现实的鱿鱼世界完全相反的 互助共创关系 。

Initiatives **&** *Tactics* 项目是一个站点网络/资源库，您正在进入本网络的其中一个站点分支。项目总述将是一个单独的结构图式站点，它目前尚未上线；上线后将出现在这个位置。
Note: 感谢 **Notrace** 、**CrimethInc**、**PrivacyInternational**、**AccessNow**，以及所有提供宝贵经验的行动者、培训师和支持者。
[image]
Disclaimer：

本项目二期工程完全致力于协助安全性的提升。
我们从未鼓励任何人采取超出能力范围的行动。
本站所有页面均服务于对安全问题和防御措施的研究、教育和自主学习，与任何动员无关。

Note: 本站点、和本项目站点网络中的所有站点，均可一键复制到您的私人账户中，并按照您需要的格式导出到本地，供离线使用。
[image]

建议使用**Tor**浏览器阅读本站。

站点总述

云舞白的新生：iyp·整体攻防总述：我们是谁、为何而来 ... 20年战略图谱

整体攻防训练框架 - 多措并举

如果是您是前线社区的新队友，或者您正在主持为新队友提供的安全知识培训工作，请从这里开始：

📚总教材-CompleteTutorial

- [image]S01整体安全 - 总章节：前线安防入门课
- [image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
- [image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

💯训练-SelfDirectedTraining 🍎心理安全-PsychologicalSecurity

- [image]S04完美隐身-总章节：机智是重要实力
- [image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

🔥反渗透/线人&减轻背叛的损失-AntiInfiltration&informant

- [image]S08精神心理安全-总章节：唤回心灵

- [image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

- [image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

❤️🔥行动安全性-OPSEC

- [image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训

- [image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

🎀人际安全&关系结构革命-RelationshipsRevolution

- [image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会

- [image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放

- [image]S11关系结构革命-总章节

💝组织、照护和互助 - Organizing&SelfCare&MutualAid

- [image]S12我盟-总章节

- [image]S13互助生存-总章节：共生的自由状态

💼操作安全性 - Digital Security 📦技术哲学和技术直觉-Intuition&PhilosophyofTech

- S14培训师指南 - 总章节

📌纸条 □工具-Tools

威胁知识库 - 知己知彼

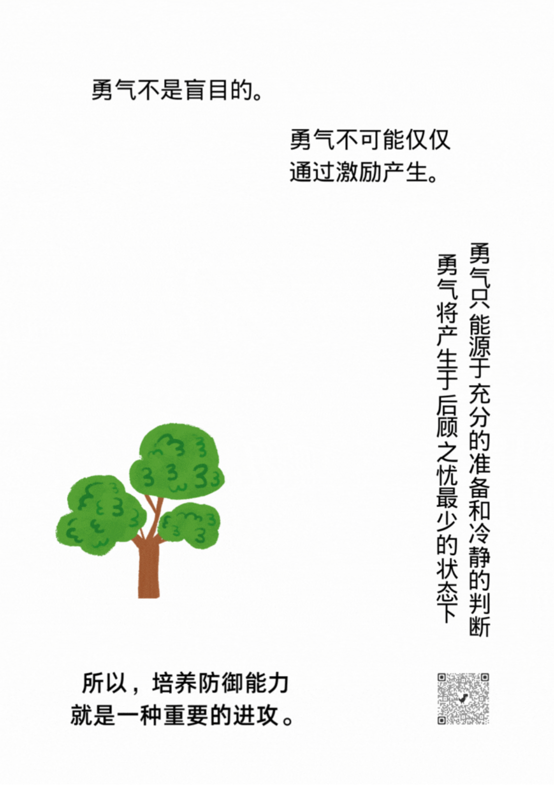
如果您认为自己已经准备好了，请从这里开始：

威胁知识库-索引页

☠镇压手段

⛑自卫措施

[image]带有攻击树的威胁库用例示范



[image]

📚 总教材-CompleteTutorial

💡

> 战士不应依赖运气，而应依靠准备。

—— 山本常朝

💯 训练-SelfDirectedTraining

[image]

正视所有恐惧、愤怒和不适，然后才能建设性修正。

Amateurs practice until they get it right, professionals practice until they can’t get it wrong.

🔥 反渗透/线人&减轻背叛的损失-AntiInfiltration&informant

[image]

不幸的是，与寻常的理解完全相反 —— 被镇压系统瞄准事实上是一种巨大的失败，绝非“成功”；如果必需衡量“价值”的话，我们每个人都应该致力于对我们自己的战略、对我们自己的战友和政治理想“具有越来越大的价值”，而不是对敌方的维稳指标有价值！这两种价值恰恰相对立。

也建议您 警惕 那些喜欢吹嘘自己的“敏感级别”或过往功绩的人，这至少意味着此人要么并不了解前线的生存策略和价值判断，要么，可能是在钓鱼。

🍎 心理安全-PsychologicalSecurity

[image]

孤独可能是最大的风险因素。

“孤独”不完全指孤军奋战；更有，如果你随时需要拿出一部分精力来防备周围人（不论原因如何），你就很容易筋疲力尽，进而导致出错。

这种状况的可能性与您的工作的激进程

度成正比。我们称之为“心理安全”。

心理安全是防御工事中的重要部分，毕竟“事在人为”，再精良的武器、再绝妙的战术设计，都不如一副理智机敏的头脑。

组织、照护和互助-Organizing&SelfCare&MutualAid

[image]

一个不爱你的人什么都能做得出来。或者说，他们对你做出什么都不会令人惊讶。

我们需要彼此间的爱才能实现互相信任和依赖，才能做到危难之时彼此照应相依为命。

不论你为自己打造多大的“可利用价值”都不足以给你这样的安全感，相反，那只会让你始终处于随时可能被取代的恐慌中。

只有爱，才是无可取代的。

人不是工具，我们不是彼此的玩偶，这是我们的组织结构区别于全球资本主义社会大环境的根本。

操作安全性-Digital Security

"永远不要把思想和行动分开，不要把我们知道的东西、我们理解的东西和我们做的东西、我们采取行动的东西分开"。
—— 阿尔弗雷多·M·博南诺

总教材-**CompleteTutorial**

[image]

Name

[image]如何不暴露手机号、不花钱，实现双因素身份验证？
[image]Telegram的隐私保护指南，和信息搜索工具
[image]自我人肉
[image]他们如何抓捕说真话的人？灾难和教训
[image]如何检查您的VPN连接是否实际加密
[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话
[image]如何检查MacOS上的恶意软件和键盘监听程序
[image]如何保持 Android 设备免受警察的侵害
[image]如何识别手机上的恶意软件？
[image]在线组织和互助需要多方面小心以维护所有参与者的安全：基本注意事项
[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？
[image]如果您的手机被盗或被警察抢走...
[image]什么是凭据填充攻击？如何选择密码管理器？
[image]一句话安全须知：记住这些句子，以简单地优化您的安全性
[image]如何才能安全地使用端对端加密（比如Signal）：准则
[image]如何跨社交媒体平台追踪目标人：对抗性思考方式
[image]使用Tor保护自己时千万不要做这9件事
[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式
[image]攻击加密系统的多种形式和防御方法
[image]简易分身术：妥善管理您的在线身份并获得安全的方法
[image]给活动家的反人肉指南
[image]如何知道有人正在线人肉你？6个简单的方法
[image]袜子木偶 - 分身创建的小技巧
[image]泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？

[image]社交媒体上的行动主义安全性:框架手册
[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗
[image]在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作
[image]攻击者如何收集有关目标的情报？他们能了解你多少？
[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式
[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则
[image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击
[image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民
[image]这些使用暗网的人是如何被抓到的？: 总结教训
[image]当您准备像编程随想那样工作...：须知
[image]移除你的绵羊墙：给普通人的5个防御课程
[image]如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？
[image]设备好像被黑了怎么办？ - 数字急救包

🎀 人际安全&关系结构革命-RelationshipsRevolution

[image]

“你是谁？” - 这个问题的答案往往只是由一大堆 身份 拼凑而成。这就是导致我们之间难以切实连接的根本性错误。

导致人 被工具性评估 。导致关系

以结果为导向 ，并因此充斥着始终无法满足的愤懑。

无政府主义革命正是在致力于构建一种关系结构，在这种关系中，没有任何人能够系统性地支配或压迫他人，因为权力分配均匀，合作比残酷的竞争更有激励作用。
它就是 威权主义的对立面 。

总教材-**CompleteTutorial**

[image]

Name

[image]是什么导致队友间不分享知识？
[image]建立国际团结：全球斗争中的人际关系
[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image]是否有比米兔更好的解决方案？如何？ ：超越米兔S09E01
[image]恢复团结：超越米兔S09E02
[image]直击性骚扰和性侵犯的根本：超越米兔S09E03
[image]为我们自己负责 - 打破反贼圈子中关于攻击和虐待的僵局：超越米兔S09E04
[image]搬弄权力 - 性癖好与虐待的本质区别 ：超越米兔S09E04
[image]社群集体如何帮助私人亲密关系中出现的问题？ ：超越米兔S09E05
[image]“我的”朋友还是“我们”的朋友？ ：如何执行担保措施
[image]S10战友爱侣 - 总章节:

爱，关系，嫉妒，拒绝和解放
[image]性、婚恋、密友…“反贼”如何构建亲密关系：战友爱侣S10E01
[image]杀猪盘和可利用的同理心：战友爱侣S10E02
[image]亲密关系中的权威主义：战友爱侣S10E03
[image]所谓的“开放关系”可能并不是你想的那种…：战友爱侣S10E04
[image]关系无政府状态的伦理学：战友爱侣S10E05
[image]无界，无级，无限，无尽…… 无忧，自带安全感的亲密关系：战友爱侣S10E0N-1
[image]构建没有内耗的爱：把我们的亲密关系从资本主义逻辑的泥潭里拯救出来 - 战友爱侣S10E0N
[image]S11关系结构革命-总章节
[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01
[image]社区应该是什么，是谁在玩坏这个概念：关系结构革命S11E02
[image]解放结构：关系结构革命S11E03
[image]如何与内部冲突共存
[image]如何组织社交空间
[image]结识新认识的人时您应该曝光自己多少信息？- 原则和技巧
[image]在这个操蛋的世界里，奋力地相爱！—— 情人节2026
[image]在激进左翼亚文化中恢复团结：关系结构革命 S11E0N＋1
[image]创意干预工具包：制止人际暴力实用指南 - 关系结构革命S11E0N

❤🔥 行动安全性-OPSEC

[image]

放下功利心名利欲的那一刻，您就提升了至少一半的安全性。这绝非笑谈。

在下一波激烈的街头浪潮来临之前 —— 学习如何制作和使用盾牌、加固横幅，如何保护自己和队友免受橡皮子弹、水枪、警棍、胡椒喷雾、监视和大规模抓捕的攻击。

防御能力是所有行动的持续性基建。

日常练习。熟能生巧。让您和队友习惯于安防措施和机动性的完美契合，你们就可以快速抓住任何机会窗口。

总教材-**CompleteTutorial**

[image]

Name
行动安全性总述
[image]在线组织和互助需要多方面小心以维护所有参与者的安全：基本注意事项
[image]在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作
[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则
[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
[image]直接行动分步指南：它是什么、它有什么用、如何获得成功
[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训

[image]认识警棍，危害能力和防御方法：街头实战指南 S05E01
[image]头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02
[image]抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03
[image]如何处理枪伤：街头实战指南 S05E04
[image]从雨伞到激光、气球到电动工具：街头实战指南 S05E05 - 战术器具综述
[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06
[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07
[image]了解防弹衣：街头实战指南 S05E08
[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09
[image]了解防暴弹药，以及如何保护自己 ：示威参与者指南 S05E10
[image]让监视摄像头失明：示威参与者指南S05E11
[image]在街上保持安全：街头实战指南 S05E12
[image]和媒体说话时如何避免陷阱：街头实战指南 S05E13
[image]加固横幅和盾牌的制作和使用方法：示威参与者指南 S05E14
占领街头：封锁和阻断指南 - 街头实战指南 S05E15
[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16
[image]反击, 保持自由：街头实战指南 S05E17
[image]S04完美隐身-总章节：机智是重要实力
[image]直面你的对手 - 6大原则：完美隐身S04E01
[image]了解追踪者的手段和你的弱点：完美隐身 S04E02
[image]思考方式是战略性的：完美隐身 S04E03
[image]技术增值部分-最简单的分身方法：完美隐身 S04E04
[image]清扫和清点-信息篡改的重要步骤：完美隐身 S04E05
[image]令人兴奋的心理过招：完美隐身 S04E06
[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A
[image]大清洗 - 扫荡危险区域：完美隐身 S04E07
[image]街头搏击基本技巧（转帖）
[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image]抢先采取行动 - 反侦基础课 S06E01：七点规则和态势感知

[image]准确的情报和判断 - 反侦基础课 S06E02: 确立基准线
[image]您必备的基本防身装备：反侦基础课 S06E03
[image]如何摆脱手铐、绳索、束线带和布基胶带：反侦基础课 S06E04
[image]如何撬锁、翻栅栏、短路点火发动汽车：反侦基础课 S06E05
[image]特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06
[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A
[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C
[image]如何欺骗，和如何防骗：反侦基础课 S06E07
[image]武器和自我防御的重要策略：反侦基础课 S06E08
[image]如何在大规模枪击案中幸存：反侦基础课 S06E09
[image]如何检测您是否正在受到监视：监视检测和特殊保护行动
[image]暗中监视的迹象
[image]如何安全地留住证据：给真相的记录者一些技术技巧建议
[image]给公民记录者的技巧指南
[image]公民取证技巧：如何留住真相？
[image]当你手握真相：最基本的防护知识
[image]在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学S07E05
[image]什么是伪装，如何伪装，如何识破 — — 社交工程攻防基础
[image]如何识别抗议活动中可见的和不可见的监视
[image]如何躲避无人机 - 监视时代须知
📱警察如何利用抗议者的手机追踪每个人
[image]您是否正在被 AirTag 跟踪？这里是检查方法
[image]空中监视如何追踪抗议者？
[image]当您准备参加抗议活动：基本指南
[image]5种常用的“击落”无人机的方法
[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事
[image]直接行动的关键在于协作，但协作的能力并非天生
[image]宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切

📌 纸条-Notes

[image]

二期工程“纸条”专栏中收纳的洞见大多来自本站首轮共创合作者，以及他们的地方伙伴。

本项目一期工程中的同名专题旨在收纳理论/原理相关的见解；二期工程则欢迎更多闲聊和静思。

总教材-**CompleteTutorial**

[image]

Name
🚶 不是“个人问题”
🍻你在人际关系处理方面遇到过哪些尬事？贴张便签，我们聊聊
[image]安全文化和广阔的生活
[image]本质主义和身份政治问题
[image]街头政治对抗技巧提示（就是打架）
[image]解放教育101:如何培育潜在的同道
[image]精英主义语言的问题 - 与激进派中产阶级活动家一起探讨
[image]如何选战友
[image]需要解决方案，而不是恐惧
[image]技术与权力
[image]走出部落
[image]我们需要更诚实地思考如何组织
[image]警惕镇压者通过诈骗在你的设备上安装间谍软件：来自意大利的教训
[image]转帖：从艾未未回国，反思互联网的“伪”影响和流量魔咒
[image]转帖：关于近日再现的街头镇压毒气弹（传闻可能不准）

技术哲学和技术直觉-Intuition&PhilosophyofTech

[image]

对于安防的目标来说，您不需要读懂代码。就如您不需要拿下土木工程学博学学位也能避免掉进坑里。技术的底层逻辑是政治哲学，就如万有引力，它解释了任何一种“坑”的危险所在；他人的前车之鉴绝非笑柄，它揭露了挖坑人的思路和心机。

总教材-CompleteTutorial

[image]

Name
🇨🇳中国跨境数字镇压的工业化和私营承包商演变：公民实验室最新报告“Tall Tales”
[image]全球噩梦 - 跨国电信生态系统下的隐形枷锁：公民实验室调查“Bad Connection”
[image]聊天机器人的设计“初衷”就是为了让你产生妄想：这不是漏洞，而是商业模式
[image]当科技巨头走向战争…
[image]“不要再拍了！请关闭设备删除影像”
[image]超越屏幕
[image]暗中监视的迹象
[image]间谍机构使用的开源情报监视方法
□🖳自由软件的问题... 是资本主义
[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？
□地主2.0：科技的新食利资本主义
[image]你家冰箱如何作为呈堂证供？
[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证
[image]构建技术直觉：生存在数字世界必备的本能
[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证
[image]数字取证正在泛滥：政府可以从你的手机中提取哪些

数据？
[image] “智能城市”究竟是个什么鬼
[image]一些简单的措施以防止您的汽车被骇客控制
[image]如何使用社交工程来攻击 2FA？
[image]小心预览
[image]警察和间谍如何解码你的照片？
[image]你的手机如何背叛了民主？
[image]即使数据是匿名的，您的身份仍然可以被识别
[image]互联网作为新的圈地运动
[image]如何从Matrix中醒来
[image]礼貌的偏执
[image]移除你的绵羊墙：给普通人的5个防御课程

工具-Tools

总教材-**CompleteTutorial**

[image]

Name	关键词	创建时间
[image]把你的Telegram变成无限云存储	telegram 云存储 跨平台	2026年8月6日
[image]实时查看您的计算机所连接的位置	网络安全 自检	2026年8月5日
[image]噪声生成式混合网络，比Tor更胜一筹	VPN 元数据 加密 反追踪 混合网络	2026年8月4日
[image]反追踪浏览器	反追踪 数字足迹 浏览器	2026年8月3日
[image]自托管AI会议助手	AI 会议 组织 自托管	2026年7月31日
[image]安全的文件存储与共享	存储安全 文件处理 查询整理 管理	2026年7月27日
[image]随手存档	存档 管理	2026年7月24日
[image]离线图像压	离线 管理	2026年7月23日

缩工具		
[image]开源情报工具库2026	对抗性思考方式 开源情报 独立调查 自检 防御	2026年7月20日
[image]安全工具箱规整 - 2026版	个人 元搜索 加密 安全搜索 工具 查询整理 清理 电脑 病毒检测 离线 移动设备 自卫 防御 预防性 高科技镇压	2026年7月17日
[image]新闻收割机	AI 新闻 生产力	2026年7月15日
[image]您的专业级私人情报终端已开源	AI 开源情报 独立调查 自助	2026年7月9日
[image]暗网调查工具：去匿名化	tor 对抗性思考方式 暗网 独立调查 自检 预防性	2026年7月8日
[image]跨平台社交媒体情报 - 追踪和自检	个人 团队 对抗性思考方式 开源情报 数字足迹 独立调查 社交媒体情报 自检 防御	2026年7月7日
[image]离线知识库：应对灾难和突发状况	AI 存储安全 战争 气候灾难 离线 自助 预防性	2026年7月6日
[image]隐私堡垒门罗币 - 服务清单2026：钱包、交易所、匿名SIM卡、主机及其他	SIM匿名 加密货币 自托管 门罗币 隐私	2026年6月29日
[image]在不安全渠道上尽可能安全地共享秘密	传输安全 加密	2026年6月26日
[image]隐私安全型开源家庭服务器	存储安全 服务器 网络攻击 自主 隐私	2026年6月24日
[image]注重隐私的智能手机	硬件 移动设备	2026年6月15日
[image]监视资本主义之外的元搜索引擎	元搜索引擎 开源情报 自托管 隐私	2026年6月10日
[image]Veilid 网络上的匿名私密通信工	IMs P2P Veilid 匿名 团队	2026年6月9日

具		
[image]自托管黑头套紧急响应	个人 威胁响应 强迫失踪 自助 预防性	2026年6月8日
[image]文件上传恶意软件扫描	恶意软件 数据安全 病毒检测 自检	2026年6月2日
[image]有人在悄悄监视你吗？	个人 反监视 智能眼镜 自卫 街头	2026年5月29日
[image]3D资源库	3D	2026年5月27日
🏡家庭管理	团队 管理 自托管	2026年5月26日
[image]清除电脑上的取证痕迹	数字取证 电脑 自检 预防性	2026年5月25日
[image]翻译视频	AI 翻译 语音识别	2026年5月22日
[image]从数据库中自动生成美观易读的ER图（给本项目二期工程培训基地参考）	实体关系图 数据处理 数据库	2026年5月15日
[image]基于人工智能的暗网开源情报工具	AI 开源情报 暗网	2026年5月14日
[image]免 KYC 的交易平台（精选）	加密货币 匿名 身份验证	2026年5月13日
[image]找信号：对抗黄貂鱼等监视设备	Wi-Fi 自卫 蓝牙 黄貂鱼	2026年5月8日
[image]看看自己在警察眼里长啥样：浏览器数据的取证分析工具	对抗性思考方式 数字取证 浏览器 自检	2026年4月29日
[image]一个适用于macOS 的反取证应用	USB 反取证 数据保护 电脑	2026年4月28日
[image]“干净”的浏览器	免追踪 浏览器 自主	2026年4月27日
📚读书和书籍管理，配AI翻译	AI 书 查询整理 翻译	2026年4月23日
[image]从普通浏览器进入Tor网络	tor 浏览器	2026年2月27日
[image]互助抗镇压	ICE 互助 反监视 突袭 自卫 镇压	2025年11月20日
[image]无云自托管	存储安全 文件处理	2025年11月4日

文件存储	端对端加密 自托管	
[image]跨平台AI翻译	AI 翻译	2025年11月3日
[image]用手机作为电脑麦克风	电脑 移动设备	2025年11月2日
[image]从100多个平台下载视频	下载	2025年11月1日
[image]本地密码管理器	加密 密码 离线	2025年10月17日
[image]2025 年 Tor 使用指南	tor	2025年10月16日
[image]网状网络通信，支持LoRa 设备	IMs 加密 离线 网状网络 通信	2025年10月15日
[image]离线安全存储 - 完全本地无需服务器	存储安全 数据安全 查询整理 离线	2025年10月14日
[image]点对点文件传输	传输安全 加密 数据安全	2025年10月13日
[image]戴面具的电邮	免追踪 电邮	2025年10月10日
🗒文件转换器 - 开源、完全本地化不用云，永久免费	文件处理	2025年10月9日
📍与可信赖的朋友安全地共享位置	团队 定位 端对端加密	2025年10月8日
□2025最新的洋葱链接目录	tor 洋葱	2025年10月7日
□洋葱网站模版	暗网	2025年10月6日
[image]隐私型浏览器 - 谷歌浏览器替代品	数字卫生 数字足迹 浏览器 谷歌替代方案	2025年10月5日
[image]隐匿点/安全屋周围Wi-Fi入侵检测系统	Wi-Fi 威胁识别 安全屋 独居 网络攻击 自检 防御 预防性	2025年9月30日
[image]更安全的密码管理解决方案	PGP 密码	2025年9月26日
[image]反检测浏览器	OSINT 浏览器 网页抓取	2025年9月24日
[image]取证工具：磁盘分析和文件恢复	取证 对抗性思考方式 数据丢失 自助	2025年9月23日

[image]隐写工具	传输安全 元数据 加密 隐写术	2025年9月19日
[image]消除对Google Web 服务依赖的轻量级方法	谷歌 谷歌替代方案	2025年9月18日
☂智能眼镜隐私保护	AI 生物识别 自卫	2025年9月17日
[image]生存训练	AI 生存训练 自助	2025年9月16日
[image]开源、离网、去中心化的网状网络	传输安全 加密 离线 移动设备 网状网络	2025年9月15日
[image]做移动设备取证和数字调查的开源平台	取证 威胁响应 移动设备 自助	2025年9月12日
[image]自托管文件转换	文件处理 自托管	2025年9月10日
[image]安全的剪贴板	剪贴板 加密 存储安全	2025年9月9日
[image]谷歌“查找我的设备”的安全开源替代	开源 移动设备 谷歌 防盗	2025年9月8日
[image]将数字本文转换为手写字体	笔迹鉴定	2025年9月5日
[image]适合高风险用户的通信平台	IMs tor 加密 团队 自托管	2025年9月4日
[image]AI文档处理工具	AI 文件处理	2025年9月3日
[image]安全的虚拟浏览器	团队 浏览器 电脑	2025年9月1日
[image]开源防病毒软件精选	病毒检测 自助	2025年8月28日
[image]私密P2P的团队IM，无需服务器	IMs tor 加密 移动设备	2025年8月27日
[image]高安全度终端私密聊天	IMs 加密 电脑 自托管	2025年8月26日
[image]把手机变成临时USB记忆棒	存储安全 安卓 转储	2025年8月25日
[image]适用于移动设备的Tor浏览器精选	tor 个人 移动设备	2025年8月22日

[image]Google Drive 的开源替代产品	存储安全 开源 文件处理	2025年8月21日
[image]寻找代码中的漏洞	开发者 自检 预防性	2025年8月20日
[image]实时语音翻译	AI 无障碍 翻译 自主	2025年8月19日
[image]强制加密密钥 USB 存储	存储安全 身份验证	2025年8月13日
[image]终端上的 AI Agent	AI 个人	2025年8月12日
[image]安卓隐私浏览器	安卓 数据最小化 浏览器 移动设备	2025年8月11日
[image]加密的安卓位置共享	tor 加密 安卓 定位 移动设备	2025年8月8日
[image]安卓 - 简单易用的隐私管理器	安卓 移动设备 自助 预防性	2025年8月7日
[image]专为保护您的照片而设计的相机应用	传输安全 加密 反审查 存储安全 移动设备 预防性	2025年8月6日
[image]在 Docker 中运行 macOS虚拟机	电脑 虚拟机	2025年8月5日
[image]自检URL阻止恶意网站	病毒检测 监测 自检	2025年7月27日
[image]Telegram内容提取工具	IMs OSINT telegram 查询整理	2025年7月24日
[image]离线求救	个人 气候灾难 自助	2025年7月18日
[image]像1984那样通信	反封锁	2025年7月16日
[image]绕开KYC 的情况下用加密货币交换加密货币的方法	加密货币 身份验证	2025年7月13日
[image]带有频道功能的离线P2P安全通信	IMs P2P 加密 团队 离线	2025年7月11日
[image]一些安全存储照片的方法 [Android版]	存储安全 安卓 自主 自托管	2025年7月11日
[image]安全文件存	加密 查询整理	2025年7月4日

储		
[image]云存储文件管理	云存储 查询整理	2025年7月3日
[image]Telegram 语音笔记转录和摘要机器人	telegram 效率	2025年7月2日
[image]安全的秘密共享	传输安全 加密	2025年6月23日
[image]极简发布平台	倡导活动	2025年6月18日
[image]看视频学外语	AI 学习	2025年6月10日
[image]去中心化 P2P 聊天应用	IMs P2P 加密 去中心化	2025年6月6日
[image]清除 Windows 11 中所有垃圾	反侦察 电脑	2025年5月22日
[image]隐私设置终极指南	自助 预防性	2025年5月16日
[image]将电子书转换为有声读物	倡导活动 效率	2025年5月15日
[image]匿名 SIM/SMS 服务	SMS 免追踪 加密	2025年5月9日
[image]在视频中嵌入隐藏水印	AI 效率	2025年4月22日
[image]在本地运行 AI	AI 自托管	2025年4月17日
[image]免费下载工具	效率	2025年4月15日
[image]创建和注入浏览器指纹	免追踪 对抗性思考方式 浏览器	2025年4月14日
[image]交互式高质量网页存档	查询整理 浏览器	2025年4月11日
[image]命令行隐写工具	加密 隐写术	2025年4月8日
[image]去中心化无服务器的匿名聊天	IMs 加密 去中心化 浏览器 自托管	2025年3月26日
[image]URL 检查	URL 免追踪 预防性	2025年3月25日
[image]适用于多媒体的跨平台搜索引擎	元数据 查询整理 跨平台	2025年3月22日

和文件资源管理器		
[image]安卓下载器：下载音视频文件	安卓	2025年3月19日
[image]加密、生成校验和销毁文件	加密 查询整理 身份验证	2025年3月18日
[image]将操作系统映像写入USB	安卓	2025年3月17日
[image]在不同操作系统之间传输文件	IMs 传输安全 加密	2025年3月13日
[image]使用临时网络命名空间通过VPN 运行应用程序	代理	2025年3月12日
[image]定性清理硬盘	反侦察 彻底擦除 自主 预防性	2025年3月10日
[image]来自 GitHub的AI工具目录	AI	2025年1月5日
[image]安卓文件管理和清理工具	反侦察 安卓 查询整理	2025年1月4日
[image]安全IMs	IMs tor 传输安全 加密	2024年12月17日
[image]给Tor网络研究人员的小工具	tor	2024年12月10日
[image]备份/恢复工具	加密 备份 数据丢失	2024年12月3日
[image]轻量级的高效隐写工具	隐写术	2024年11月25日
[image]匿名托管服务VPS	匿名托管 反封锁 自助	2024年11月21日
[image]开源加密工具	加密 文件处理 查询整理 预防性	2024年11月20日
[image]安卓的网状网络解决方案	安卓 离线	2024年11月19日
[image]开源跨浏览器管理器	效率 浏览器	2024年11月15日
[image]一些工具都可用来恢复已删除的文件	反侦察 对抗性思考方式 数据丢失 自助	2024年11月15日
[image]伪造手机位置	免追踪 定位 自助	2024年11月14日
[image]使用容器隔	tor 沙箱 虚拟机 预	2024年11月14日

离应用程序和虚拟机	防性	
[image]备份和恢复已删除的文件	数据丢失	2024年11月13日
[image]去除图像中的水印和其他元素	元数据 数字足迹 自助	2024年10月22日
[image]安全存储照片和视频	传输安全 加密 反侦察	2024年10月14日
[image]完全Tor	tor	2024年10月10日
[image]去中心化的社交网络协议	去中心化 社交网络	2024年10月8日
[image]一系列免费的人工智能翻译器	效率	2024年9月24日
[image]开源剪贴板管理器	剪贴板 效率	2024年9月6日
[image]从明网搜索Tor	tor	2024年9月3日
[image]隐私型电邮提供商的列表	免追踪 加密 暗网 电邮	2024年8月30日
[image]检查密码是否泄漏	密码 自检	2024年8月24日
[image]安全消息应用	IMs 加密 身份验证	2024年8月23日
[image]硬件密码管理器	密码 身份验证	2024年8月19日
[image]一些私密安全的文件传输解决方案	传输安全 加密	2024年8月8日
[image]更安全的实时视频会议平台	团队 效率	2024年8月6日
[image]开源协作式书签管理器	云存储 团队 自托管	2024年8月5日
[image]安全存储和身份验证管理	2FA 密码 身份验证	2024年7月29日
[image]以更私密简洁的方式浏览Twitter/X	免追踪 社交网络	2024年7月26日
[image]开源 2FA 应用	2FA 加密 密码	2024年7月25日
[image]安卓开源短信网关	SMS 安卓 移动设备	2024年7月18日

[image]安全地隐藏和加密文件	传输安全 加密 反侦察 隐写术	2024年7月15日
[image]隐私型安卓网页浏览器	免追踪 安卓 数字足迹 浏览器 移动设备	2024年7月11日
[image]临时电邮	免追踪 电邮	2024年7月1日
[image]自动检查病毒，并替换为安全版本	病毒检测 自主	2024年7月1日
[image]在任何聊天工具中发送算对端加密信息	IMs 传输安全 加密	2024年6月27日
[image]完全本地化的开源密码保管	加密 安卓 密码 自托管	2024年6月24日
[image]安全共享	传输安全 加密	2024年6月21日
[image]安卓加密图库	加密 安卓 查询整理	2024年6月19日
[image]对文件中的敏感数据匿名化	反侦察 预防性	2024年6月17日
[image]去除图像中的水印和其他元素	数字足迹 自助	2024年6月15日
[image]一次性密码和2FA应用	2FA 防御	2024年6月13日
[image]加密和匿名发送文件	云存储 传输安全 加密	2024年6月11日
[image]也是隐写：将敏感信息隐藏在图像中	加密 隐写术	2024年6月7日
[image]通过临时Wi-Fi 在设备间离线传输文件	传输安全 加密 电脑 移动设备	2024年5月27日
[image]广告拦截	免追踪 浏览器 自助	2024年5月21日
[image]分析蓝牙环境是否安全	反侦察 安卓 监测 自检 防御	2024年5月17日
[image]视频隐写术	传输安全 加密 隐写术	2024年5月16日
[image]在纯文本中隐藏不可见的信息或水印	传输安全 隐写术	2024年5月15日
[image]安全备份工具	加密 备份 数据丢失 查询整理 自托管	2024年5月15日

[image]安卓加密短信	传输安全 加密 安卓 移动设备	2024年5月9日
[image]从视频或音频中总结对话	效率	2024年5月9日
[image]开源零知识加密文件共享	传输安全 加密	2024年4月25日
检查可疑电子邮件、链接和文件的在线工具	URL 电邮 病毒检测 自助	2024年4月23日
[image]把您的所有消息应用整合在一处	IMs 加密 效率 自托管	2024年4月19日
[image]洋葱路由功能的安全信息传递系统	tor 传输安全 免追踪 加密	2024年4月15日
[image]一套鼠标和键盘控制多台计算机	开源 效率	2024年4月9日
[image]将安卓手机连接到电脑	传输安全 加密 安卓	2024年4月3日
[image]本地托管的PDF操作工具	密码 查询整理 自托管	2024年3月26日
[image]开源笔记应用跨平台	离线 笔记	2024年3月22日
[image]免费的去中心化社交网络平台	去中心化 社交网络	2024年3月20日
[image]替换掉那些不够安全的插件	免追踪 开源 浏览器	2024年3月19日
[image]安卓文件管理器	安卓 查询整理	2024年3月18日
[image]端对端加密笔记	P2P 加密	2024年3月14日
[image]免费读书	信息民主化 海盗	2024年3月11日
[image]在坏人强行访问您的设备的情况下抹除数据	反侦察 移动设备 自助 预防性	2024年3月6日
[image]打破付费墙	付费墙 信息民主化	2024年1月29日
[image]为孤军奋战者准备的预警方案	反间谍 强迫失踪 报警 独居 自助 防御 预防性	2024年1月17日
[image]安全地存储秘密	QR码 传输安全 加密	2024年1月12日

[image]浏览器中的流媒体工作室	效率	2023年12月23日
[image]一系列隐写工具	传输安全 加密 隐写术	2023年12月19日
[image]隐私自助：流行产品的开源替代品目录	免追踪 反侦察 安全搜索 数字足迹	2023年12月14日
[image]一些可选的翻译服务	个人 团队 效率	2023年12月8日
[image]一些注重隐私的浏览器扩展	数字足迹 电脑 预防性	2023年12月6日
[image]绕开面部识别	免追踪 防御 预防性	2023年11月29日
[image]基于云的多用户 Chrome 浏览器	团队 效率	2023年11月13日
[image]访问网站时保护自己的敏感数据	URL 免追踪 自助	2023年11月9日
[image]Tor工具系列	tor 反封锁 安全搜索 暗网	2023年11月6日
[image]保护安卓手机免受警察的抢夺	反侦察 安卓 移动设备 自助 防御 预防性	2023年10月26日
[image]将手机变成电脑麦克风	电脑 移动设备	2023年10月20日
[image]无限制传输任何大小的文件	P2P 传输安全	2023年10月19日
[image]安全浏览器	代理 免追踪 反封锁 反间谍 数字足迹 预防性	2023年10月17日
[image]将整个网站转换为PDF	反封锁 查询整理	2023年9月22日
[image]一次性加密笔记	传输安全 加密 阅后即焚	2023年9月21日
[image]Telegram探索工具	OSINT telegram 安全搜索	2023年9月12日
[image]自动检测链接是否安全	URL 病毒检测 预防性	2023年8月10日
[image]点对点的匿名安全通信	IMs P2P tor	2023年8月8日
[image]通用安卓卸载器GUI	安卓 清理	2023年7月18日

[image]一个功能强大的自托管 Internet 存档解决方案	文件处理 查询整理 自托管	2023年7月17日
[image]离线安全传输	传输安全	2023年7月4日
[image]在不安全的渠道上安全传输	传输安全 免追踪 反审查	2023年7月3日
[image]安全的即时通信工具 Speek	IMs 免追踪 加密 去中心化	2023年6月22日
[image]创建个人 VPN	代理 反审查 反封锁 自助	2023年6月21日
[image]提高安卓设备隐私和性能的工具	反封锁 安卓 沙箱	2023年6月19日
[image]安全搜索	元搜索 免追踪 安全搜索	2023年5月31日
[image]对URL进行加密和解密	URL 传输安全 加密	2023年5月26日
[image]取证和反取证工具及资源	取证 对抗性思考方式 自检	2023年5月13日
[image]成为自己的邮件服务提供商	电邮 自托管	2023年4月12日
[image]设备间安全地同步剪贴板	传输安全 加密 电脑 移动设备	2023年3月22日
[image]用于去中心化网络的自托管轻量级通信工具	IMs 加密 去中心化 自托管	2023年3月21日
[image]安全打开陌生的缩短链接	URL 自助 预防性	2023年3月20日
[image]移动网络浏览器绕过互联网审查	反封锁 移动设备	2023年3月18日
[image]VirusTotal 的官方浏览器扩展	病毒检测 自检	2023年3月12日
[image]GPS工具	定位	2023年3月6日
[image]在手机上隐藏私密文件和应用	反侦察 安卓 预防性	2023年3月3日
[image]P2P信使	IMs P2P 加密	2023年2月27日
[image]创建一个加密的相册	加密 移动设备	2023年2月9日
[image]专注于隐私的安卓网络浏览器	免追踪 安卓 移动设备	2023年2月8日

[image]在Android上加密文件	加密 安卓 密码	2023年2月1日
[image]一些可以欺骗智能手机上的地理位置数据的工具	免追踪 对抗性思考方式 移动设备	2023年1月30日
[image]私密电话号码	SMS 手机号 自主 身份验证	2022年12月2日
[image]可自托管的匿名pastebin	传输安全 加密 自托管 阅后即焚	2022年11月26日
[image]一些较安全的电邮客户端选项	加密 电邮	2022年11月25日
[image]一系列安全的即时通信软件和服务	IMs P2P tor 传输安全 免追踪 去中心化	2022年11月23日
[image]开源电邮客户端	传输安全 加密 电邮	2022年11月22日
[image]将任何网站变成PDF文件	反封锁 查询整理	2022年11月19日
[image]安全的云中存储	云存储 元数据 加密 查询整理 自托管	2022年11月18日
[image]调查区块链上的交易	加密货币 自检 预防性	2022年11月17日
[image]一些匿名的电邮选择	免追踪 电邮	2022年11月15日
[image]检查您的代理是否真的起到保护作用	代理 自检	2022年11月3日
[image]加密文件管理	加密 查询整理	2022年11月2日
[image]安全笔记管理	加密 反侦察	2022年10月31日
[image]插拔传输代理工具	代理 免追踪	2022年10月30日
[image]恢复误删除的数据	数据丢失 自助	2022年10月29日
[image]也是隐写	传输安全 隐写术	2022年10月23日
[image]Tor上的加密邮件服务	传输安全 暗网 电邮	2022年10月21日
[image]开源点对点社交网络	反封锁 电脑 社交网络 移动设备 自托管	2022年10月18日

[image]在安卓上隔离老大哥程序	反间谍 安卓 沙箱 自助 预防性	2022年10月11日
[image]临时/一次性电子邮件服务选项	免追踪 电邮	2022年10月9日
[image]一系列安全工具	代理 传输安全 免追踪 自助	2022年10月4日
[image]在断网后保持通信	反封锁 移动设备	2022年10月2日
[image]匿名偏执狂的选择	代理 免追踪 暗网	2022年9月29日
[image]安卓系统防火墙	安卓 防火墙	2022年9月28日
[image]类似YubiKey的虚拟USB设备	2FA 密码 预防性	2022年9月26日
[image]隐藏一个应用程序	反间谍 移动设备 预防性	2022年9月22日
[image]免费Matrix消息应用	传输安全 加密 去中心化 移动设备	2022年9月21日
[image]检查二维码是否安全	QR码 自助 预防性	2022年9月19日
[image]远程摄像机/对讲机	传输安全 安卓 独居监测 移动设备	2022年9月8日
[image]检查一个网站的安全性	病毒检测 自助 预防性	2022年8月28日
[image]安全地存储文本(消息、登录凭据、密钥、笔记...)	传输安全 加密 反侦察 自助 隐写术	2022年8月26日
[image]快速构建一个假名账户	免追踪 反侦察 自助 预防性	2022年8月25日
[image]隐藏秘密信息	传输安全 移动设备 隐写术	2022年8月24日
[image]安卓恶意软件扫描器	安卓 病毒检测 移动设备 自助 自检	2022年8月20日
[image]如果你被迫解锁手机，应该怎么做	反审查 反间谍 密码 自助 预防性	2022年8月19日
[image]如果您的手机被盗了或被警察抢走了，怎么办	免追踪 反间谍 数据丢失 移动设备 自助 预防性	2022年8月19日

[image]在断网的情况下保持联系	传输安全 反封锁 移动设备 预防性	2022年8月13日
[image]加强电子设备防盗水平	反侦察 数据丢失 电脑 移动设备 预防性	2022年8月6日
[image]快速检查可疑程序	病毒检测 自助	2022年8月3日
[image]在没有数字足迹的情况下发送秘密信息	传输安全 免追踪 加密 数字足迹	2022年8月2日
[image]方便的隐私套件	免追踪 自助	2022年7月27日
[image]隐私导向的YouTube界面	免追踪 反审查	2022年7月26日
[image]对您的电脑上的文件夹进行加密	加密 文件处理 电脑	2022年7月21日
[image]检查您的密码是否被泄漏了	密码 自检 预防性	2022年7月20日
[image]免费的macOS清洁软件	清理 电脑	2022年7月19日
[image]没有审查的多媒体内容管理系统	反审查 自托管	2022年7月17日
[image]简易P2P信使	IMs P2P 加密	2022年7月14日
[image]安全的保存您想要的链接	效率 查询整理 电脑	2022年6月29日
[image]读取陌生的/不受信任的USB设备	威胁识别 电脑 自检	2022年6月28日
[image]检查一个应用程序是否有恶意代码	安卓 病毒检测 移动设备 自助	2022年6月25日
[image]快速搭建自己的VPN服务	反封锁 自助	2022年6月21日
[image]匿名上传文件以在线分享	传输安全 免追踪	2022年6月20日
[image]虚拟手机号和马甲邮箱隐藏真实信息	免追踪 数字足迹 自助	2022年6月18日
[image]从照片中获取元数据的工具	数字足迹 自检	2022年6月8日
[image]恢复被删除	取证 数据丢失 电脑	2022年6月5日

的文件	自助 自检	
[image]绕开审查的浏览器	反封锁	2022年5月31日
[image]假联系人 - 保护手机通讯录	免追踪 对抗性思考方式 移动设备 预防性	2022年5月30日
[image]在线防病毒扫描器	病毒检测 自检	2022年5月21日
[image]彻底卸载	清理 电脑	2022年5月20日
[image]断网后通信：把智能手机变成“对讲机”	IMs 反封锁	2022年5月18日
[image]在没有VPN的情况下访问被屏蔽的网站	反封锁	2022年5月16日
[image]保密工具：找出是谁把您的文件或照片上传到了网络	反间谍 透明水印 防御 预防性	2022年5月15日
[image]巧妙地隐藏照片和视频	个人 反侦察 移动设备 防御	2022年5月14日
[image]制作自己的二维码	QR码 倡导活动	2022年5月13日
[image]生成假的信用卡资料使注册更安全	个人 免追踪 数字足迹	2022年5月11日
[image]防止未经授权的设备访问(老东西)	移动设备 自检 预防性	2022年5月10日
[image]物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪	住店 反间谍 独居 监测	2022年5月9日
[image]在浏览器中删除元数据	Web 元数据 数字足迹 清理	2022年5月6日
[image]手动检查一个网址是否安全	Web 病毒检测 自助	2022年5月6日
[image]删除照片中的元数据	元数据 数字足迹 清理 移动设备	2022年5月5日
[image]安全通信GNUnet Messenger	IMs P2P	2022年4月29日

[image]预防‘黑头套’	强迫失踪 自助 预防性	2022年4月28日
[image]去除图像上的水印和不可见标记	水印 清理 透明水印 金丝雀陷阱	2022年4月24日
[image]不联网文档归整	效率 查询整理 电脑	2022年4月5日
[image]检查智能手机是否感染了病毒	病毒检测 移动设备 自检	2022年3月30日
[image]计算机取证	反侦察 取证 对抗性 思考方式 电脑 自检	2022年3月25日
[image]内存清理 - 寻找文件差异	效率 文件处理 清理	2022年1月29日
[image]备份工具 Restic	加密 备份	2021年12月21日
[image]一系列元数据工具，从自我保护到有效利用	元数据 数字卫生 数字足迹 自助	2019年6月26日
⛅安全的云操作系统	云存储 自托管	2019年5月12日
[image]New Tool		
[image]New Tool		
[image]New		
[image]New Tool		

[image]

🌱 嗨，朋友！ 欢迎来到 iYouPort - Initiatives & Tactics 项目二期工程“整体攻防训练营”

Initiatives & Tactics 项目是一个站点网络/资源库（并非单一站点），

作为互助项目实践，这份成果来自我们与所有支持者、共识团体和前线社区的精心培育。

本项目是开源的。它将不断成长、不断变得更加丰盈。

始终欢迎更多同道为本项目持续添砖加瓦，无国界、不限语种。

Notion允许您一键复制整个站点到您的本地保存，可选择设置为离线查看，并随时可导出您所需要的多种格式文件，以分享、拓展、保存。

IYP's links

[image]

iyouport.substack.com

t.me/iyouport

patreon.com/iyouport

matters.town/@iyouport

mastodon.social/@iyouport_iyp

🚚 Progress of the project

2024 2025

[image]整体攻防训练营- *iYouPort - Initiatives & Tactics* < *Phase II* > [V1.3.0.20260427]

2026

🎉 敬请期待！

© 2014-2024 iYouPort Ⓐ 使用说明详见介绍页

[image]
📚

总教材-CompleteTutorial

战士不应依赖运气，而应依靠准备。 —— 山本常朝

[image]
[image]

S01整体安全 - 总章节：前线安防入门课

[image] 关键词	整体安全
[image] 关联	[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌；💯训练-SelfDirectedTraining；🔥反渗透/线人&减轻背叛的损失-AntiInfiltration&informant；🍎心理安全-PsychologicalSecurity；💼操作安全性 - Digital Security；❤️🔥行动安全性-OPSEC
[image] 创建时间	2025年3月2日
[image] **Description**	教材

📌

不论您目前处于哪个学习阶段、有或者没有任何行动预案，都不重要，只要您愿意开始保护自己，我们建议您从**S01**开始。

前线社区培训工作也建议从**S01**开始，尤其是华语区前线。

多年来在全世界范围内进行安全培训工作的人们都有一个共同的挫折，即苦于可持续性的不足。其中最突出的有两点特征：

1、很难持续地维护 —— 众所周知，随着周边和用户自身环境变化，应对策略也需要随之更新；并没有持久有效的安全策略，也没有适用于所有人的通用安全策略，更新越及时和准确，保护性就越高。

如果只有专业人士能提供并维护更新，资源耗费是显著的，且实用性并不能确保到每个人。

这就是为什么作为普通用户，一方面您经常会感觉谷歌到的热门安全建议似乎“不怎么适合”自己；而另方面，有不少多年前制作的安全教程内容相当细致，但大多已经过时，后期缺乏维护，已经不能提供帮助。非常可惜。

所以，培训工作的首要目标应该是培养学习者全方位的自主性 —— 从风险评估、威胁模型、技术逻辑、到安全方案策划和适时更新 —— 而不是背诵安全工具列表。

2、多数用户难以坚持安全操作 —— 几乎所有安全操作都在一定程度上不那么“便捷”，它要求用户对常规使用习惯进行足够的改变。

于是，能坚持采取安全策略的人基本都是已经了解如何更新策略的人，也就是从原理层面熟知其必要性的人。反之则不会。这就是为什么培训结束后没多久，很多学员又回到了以前的操作习惯，尤其常见于新学员。培训工作的能效水平很低。

所以，安全培训不应该是一个“单独”的项目 —— 不能让学员将其视为“额外的标准”；它需要能结合到具体的战略中，成为战略部署的一部分。培训教材应该突出安全思维的框架和原理，便于不同社区在采用时可以将教材进一步本地化处理，以贴合具体需要。

这就是**S01**教程所致力于的。通过采取一种全新的安全视角 —— 整体视角 —— 以最大程度上缓解上述问题。

尤其，S01教程不仅仅是一套基础训练，更重要的是它作为一套思考方式，可帮助本站中其他主题教材的学习更加容易。尤其对初学者来说。始终都是安全思考方式在指导安全操作。

IYP在相关工作中得出的主要经验可以大致总结为两条：

1、通过预示（而不是硬性指令）会有很大帮助 —— 与其一上来就组织教学工作，倒不如直接营造一个理想的空间，邀请大家“生活中其中”，在“生活”过程中找到“我们还需要学习、完善、提升”哪些部分，再针对性地教学。

“理想空间”可以是虚拟的，也可以是实体的，根据您的需求和具体条件；还可以是局部的/模拟特殊环境的，就像演习。这对社区新成员更有效，新人缺少实战经验，而实战经验大多属于隐性知识，言语描述总有欠缺。身临其境可能更容易激发学习者的主动思考。

这点在“心理安全”和人际结构安全两方面同样有效。

2、将安全纳入社区/团队文化成为其基础的一部分，远超过刻板的规范和考核流程 —— 就像洁净作为美德的文化环境那样，在您的团队中推崇安全操作的素养作为美德将是很有帮助的。

不要高高在上，尽可能不要说教，即便您的确是拥有丰富经验的资深人士。我们所注重的培训工作与通常意义上“教育”工作有一些区别，后者始终是自上而下的，且存在所谓的正确答案；培训则在很大程度上是横向的，培训师和学员彼此是战友关系 —— 为同一战略而共同努力。因为“安全”必须通过合作来实现；每个人越是深刻体悟共识合作的意义，我们所有人的安全程度就越高。

总之，本教程是一个主体框架，即不论您从哪个角度或层面上进入安全性培训和学习时，首先需要掌握的部分。

请点击下拉，选取相关练习题。

[image] 头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？

[image]S01E01-T1 反思现有的安全实践

[image]S01E01-T2 识别威胁并作出反应

[image]S01E01-T3 创伤经历如何影响您的认知

[image] “抓特务” 不是解决方案：整体安全S01E02- 威胁响应

[image]S01E02-T1 团队会议安全议题模版

[image]S01E02-T2 练习非暴力沟通和反馈

[image] 知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者

[image]S01E03-T1 周围是谁？可视化人际关系图谱

[image]S01E03-T2 绘制行为者关系图谱

[image] 夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产

[image]S01E04-T1 清点您最重要的信息资产

[image] 每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局

[image]S01E05-T1 制定检查清单

[image]S01E05-T2监测自己的压力水平

[image]S01E05-T3 确认可能遭受的所有威胁

[image]S01E05-T4 态势监测和威胁清单

[image] 草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全**S01E06 -** 开发您的能力，缓解您的脆弱性

[image]S01E06-T1 剖析每一种威胁

[image]S01E06-T2 找到弱点建设新的防御能力

[image]S01E06-T3 审核防御能力

[image] 充分的准备和应急反应同样重要：整体安全**S01E07 -** 计划是 “活的” **[image]** 安全是追求，而不是任务：整体安全**S01E08 -** 准备好进入行动

[image]S01E08-T1 大家怎么看

[image] 您需要真正的 “自己人”：整体安全**S01E09 -** 进入战斗状态 **[image]** 协调性很重要，从场内到场外：整体安全 **S01E10 -** 安全是保持战斗力的绝对必要条件 **[image]** 抗议中谨防常见危险：整体安全 **S01E11 -** 协作和互助就是战斗力 **[image]** 场内协作和场外接应同样重要：整体安全**S01E12 -** 紧急撤离和汇报评估

[image]
[image]

头疼医头是不够的：整体安全 **S01E01-** 什么是‘整体’？如何‘安全’？

[image] 关键词	个人 压力 团队 整体 防御
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月3日
[image] **Description**	教材

他们想要让我们崩溃。他们所做的一切都是以此为目标的。打破他们的目标是我们的首要任务。您的福祉本身不仅是反抗，更是一种政治上的自我赋权。

- Table of Contents

准备、探索、制定策略并采取行动
什么是整体安全
作为颠覆性和政治性的福祉
维护工作需要的社会政治空间
控制关于您的所有信息
应变能力和灵活性
个人对威胁的反应
直觉和生存反应
数字空间
创伤、压力和疲劳

[image]

S01教程是一份采用 “整体” 方法处理敏感人士（即国家暴力机器所针对的人群）的安全和保护的战略性指南。简言，这意味着，它不是分别看待数字安全、社会心理健康和组织安全进程的重要性，而是要将它们结合起来，并强调所有这些方面内在的相互关联性。

在过去，敏感人士安全措施的各个方面往往被分开处理，好像它们是孤立存在的。然而，这种人为地将安全问题中密切相关的方面切分开的做法，在很多情况下都只会严重限制人们采取综合性措施的能力，至少包括：

- 对安全的情感和社会心理方面缺乏足够的认识，往往使人们看不到潜在的威胁；相反，促进身心健康则有利于人们更容易了解自己的安全状况，看清风险所在、提升作出理性的关键决定的能力。

- 随着国家机器对异议人士和反叛者的数字监控越来越多，如果您对使用的数字技术的工作原理缺乏足够的了解，就会极大限制您准确感知周围威胁的能力。实现这种理解，并采取积极主动的决定，保护自己的数据以避免未授权的访问或监视，不仅意味着要对您的整体安全采取更全面的方法，而且还需要对威胁的来源有相对的把握，最严重的威胁更可能是高度隐秘的和难以察觉的。

- 在没有对所处环境和所面临的威胁进行细致分析的情况下，以临时的方式、或根据 “传统” 或听说的方式采取安全措施，往往会导致您作出带来虚假安全感的决定。因此，至关重要的是，要定期摸清自己所处的社会政治环境，尽可能准确地确定自己所面临的威胁，并更新可以用来捍卫我们的空间和继续以赋权方式工作的战略、工具和战术。

在处理安全和防御问题时，不仅要考虑到人身暴力的影响，还要考虑到结构性的、经济的、基于性别和体制的暴力、骚扰和边缘化的影响。这可能是国家所为，也可能是私营维稳公司、利益集团、非国家

武装团体，甚至是我们自己的社区和我们身边的人所为，这会深深影响每个人的心理健康、身体健康以及与朋友、家人和同事的关系。

对这些威胁的认识和采取的行动至关重要，只有这样，行动主义和抵抗才能持续，才能促进人们确定和实施安保战略的能力。因此可以说，在活动家中经常被认为是“自私”的自我照护，事实上是一种颠覆性的自我保护的政治行为，也是有效的安全战略和文化的基础。

您的安全战略也必须定期更新。随着周围环境的变化，将安全纳入您的工作的任务和挑战也在变化。在越来越依赖数字工具和平台开展活动的时代，情况尤其如此：电脑、手机、社交媒体、数码相机、和更多的技术解决方案已成为我们工作中不可或缺的工具，但它们也同时作为国家、武装团体、寡头公司、社区和家庭监视、身份识别和骚扰的工具，对我们不利。

因此，整体安全不仅必须包括每个人的身体、情感和精神状态，而且还必须包括我们手中的设备、口袋、包、家庭、办公室、街道和车辆中的电子信息。因此，本教程明确地将理解技术环境及其与我们的工作和安全之间的关系结合起来。

[image]

准备、探索、制定策略并采取行动

本教程整体分为四个大的部分：准备、探索、战略和行动。这四个步骤被认为是一个不断发展的周期性过程，应作为现有战略规划的一部分而定期重新审视。

- 在 准备 阶段，首先认识到，我们每个人都已经拥有并采取了安全措施、我们的个人信念和复原力来源、以及我们对威胁和危险的本能反应。鼓励大家考虑这些因素及其对群体动态的影响，必须认识到这些因素，才能以更有效的方式参与安全战略。

- 在 探索 阶段，按照一系列的步骤来分析我们的社会政治背景，

并就我们的工作和反对我们工作的人可能产生的具体威胁，得出一些结论。

- 在 制定策略 阶段，从我们发现的威胁入手，考虑如何制定安全策略来应对这些威胁，并制定具体的计划和协议，以行动维护我们的福祉。

- 通过以上这三个步骤，为第四个步骤，即 行动 做好准备：学习新的工具和策略，以便在行动中保障安全。“行动” 将包括一系列短小的、以情景为重点的指南，重点是具体的工具和战术 —— 从技术到心理以及其他方面 —— 帮助您在特别高风险的活动中保障安全。

S01教程旨在指导个人、集体或组织制定或改进安全战略的进程。希望该教程可以对以各种不同身份工作的人、也就是面对不同等级风险状况的人，都能有用，从基层维权者和社区组织者、到律师、记者、活动家、反叛者 …… 从建制派改良派，到无政府主义革命家。

虽然本教程是以线性叙述的形式编写的，并有一个建议的结构 (特别是对于刚开始将安全措施纳入战略规划的团队而言)，但您可以自由地将重点放在您认为有用的任何部分内容上。

大部分章节都附有一个或多个练习，这些练习应有助于您根据自己的情况了解相关内容。这些练习通常都可用于个人，但也可以在较大团队的培训工作中采用。还包括一些小贴士，以帮助您在团队环境中促进这些练习。

为了在一个集体或组织内有效地实施，您将需要定期和持续地为安全战略留出时间和空间，在行动主义的背景下，以群体的思考方式来处理您的安全和利益将更实用。

本教程是由安全和战略培训人员组成的编辑小组与一大批专家和人权维护者合作编写而成的；因此，其结构反映了在培训场景中使用的结构。每一节的练习都为个人或团体提供了思考的空间，以促进自我导向的整体安全实践路线，而无需外部培训和专门知识。

[image]

什么是整体安全

敏感人士的安全曾经一直被置于相当狭隘的角度上，例如保护他们不受暴力袭击、避免办公室被警察突袭抄家、努力在当局的司法骚扰中幸存、或在武装团体的威胁中保护自己等等。然而，这就忽视了许多不同的、微妙的压迫方式，也忽视了敏感人士为保护自身和工作可以采取的重要步骤。

本节将探讨福祉、各种安全战略和管理您的数字信息等概念，作为“整体”方法的基础。

作为颠覆性和政治性的福祉

整体方法将敏感人士的安全视为行动中的福祉：在继续从事工作的同时，保持身心健康和自我照护。

当权者的镇压战略在很大程度上是以令敏感人士恐惧、消沉、孤独、失去互信和联合行动的能力为目标的，他们试图给敏感人士制造一种幻觉即“反抗是一种地狱般的生活”。事实上完全相反，臣服才是地狱，反抗是摆脱地狱的途径 —— 直接行动是最好的疗愈。但敏感人士必须能主观体验到这一点，即福祉；当能做到时，它就是颠覆性的和政治性的。

为了保护敏感人士免于承受压力、疲劳、创伤和悲伤等问题的威胁，人们必须自觉和有意识地进行自我照护(selfcare)。自我照护不应被理解为一种自私的行为，而应被理解为一种自我保全的颠覆性的政治行为。

作为敏感人士，您如何在行动主义的背景下定义自己的福祉是主观

的、也是非常个人化的。它受到您的身体和思想的不同需求、面临的挑战、您的信仰（宗教、精神或世俗）、您的性别认同、利益和关系等多方面的影响。

敏感人士必须为自己确定安全感，并在此基础上在您的团体、组织和运动中建立团结和相互支持。这一步对于接下来的分析和战略制定过程至关重要，以捍卫和扩大你们在促进和捍卫人权方面的积极行动空间。

维护工作需要的社会政治空间

我们可以把对敏感人士的攻击看作是我们的对手 —— 那些不赞同我们的目标或积极反对我们的目标的人 —— 企图阻止我们继续工作的社会政治空间。这种空间可以包括实际的物理空间，也可以包括经济、社会、技术、法律或环境空间。

对安全采取有组织的办法意味着捍卫敏感人士的工作空间，最好是扩大它。

为了实现这一目标，您可以实施一些策略，通过倡导活动说服他人接受您的工作，阻止对您的攻击，或者可以用这些策略保护自己。本指南将探讨一些可以帮助敏感人士实施这些战略的工具和策略。

控制关于您的所有信息

正如我们曾经强调过的，“所有信息都是战略性的”，这不仅适用于国际关系，也适用于个人安防。有组织的整体安全方法需要有组织的信息和数据管理方法。尽可能保护您的所有数据 —— 您管理的文件、电子邮件和移动电话通信等等一切 —— 现在比以往任何时候都更加重要。

由于在人权活动中越来越多地使用数字技术，您的对手和他们构成的威胁也适应了这种新环境。敏感人士必须有意识地识别和保护自己的

数据，这不仅是一种安全措施，也是一种政治上的自我赋权行为。

因此，建议将整体安全做法视为保护敏感人士、和其家庭和社区的福祉和媒介，方法是始终如一地使用各种工具和策略，以相互支持和加强的方式促进心理-社会、身体和数字的安全。

将整体安全称为 “行动中的福祉”，意味着将安全视为赋权的来源。

[image]

应变能力和灵活性

应牢记的是，作为反抗者 - 统治者的对手，我们所面临的威胁和挑战总是不断变化的。在我们的工作中，“意想不到”的事件是常态，没有任何单一的安全计划能在任何情况下都奏效。我们需要对突发事件有所预期，并保持 “在场”、参与和专注，以磨练我们的应对能力。

接受我们无法让自己在任何情况下都百分百 “安全” 的事实，您还需要建立自己的复原力和灵活性。

从这个意义上说，复原力是指从挫折或伤害中迅速恢复的能力；灵活性是指针对新的或正在出现的威胁迅速采取新的安全做法的能力。

因此，您的目标肯定不是为了安全而停止工作和活动，而是减轻和减少您可能面临的威胁，在开展工作时保护您自己和您的社区。

对大多数敏感人士来说，复原力和灵活性的概念并不新鲜，拥有在危险工作中保持安全的工具和策略的想法也不新鲜。在制定新的安全办法之前，值得通过完成以下练习来探讨您现有的一些做法是否恰当：

[image]

个人对威胁的反应

制定有用的安全战略在很大程度上取决于我们的认知 —— 我们需要首先能够识别和分析威胁，才能实施避免或减少威胁的方法。

但是，基于环境、经验和许多其他因素，我们每个人对周围世界的感知都不完全相同。因此，感知有时会受到阻碍：对某些人来说显而易见的威胁可能会被其他人忽视；同样，我们也需要能够区分真正可能发生的威胁和我们错误感知的威胁，即所谓的 “毫无根据的恐惧”。

建议您熟悉影响您对威胁感知的因素，并分析在安全规划中考虑这些因素的方法。

直觉和生存反应

我们人类都有在进化过程中形成的自然保护机制 —— 其中许多机制一直都在运行中，即使没有意识到。一个常见的例子就是直觉：当直觉发出不可靠或危险的信号时，往往是因为感官已经捕捉到了多种微妙的迹象，这些迹象超出经验中对 “安全” 的判断指标。迹象本身并不能确定某个特定的威胁，但多个迹象综合起来却强烈暗示您可能处于危险之中。

这种直觉会产生焦虑，导致您要么采取直接行动以保护自己，要么寻求更多的信息来确定自己是否真的处于危险之中。

根据您发现的具体情况，这种焦虑可能会发展成恐惧，引发一种或多种生存反应。这些求生反应 —— 常见的例子包括 “僵持”、”逃跑”、伪装或战斗等等 —— 往往在您感觉到有直接危险的时候启动，很多行为就会变成下意识的，而且更难控制。

您将由此变得更快、更强、更专注。因此，这些生存策略在很多情况下都非常有效。

然而，情况并不总是如此：重要的是要认识到，我们并不总是能够控制自己对眼前危险的反应，并且应该谨慎地将这些情况下自己的反应归咎于自己或他人。

数字空间

即使您可能才开始发展自己的有组织的安全方法，但知道您的自然生存机制一直在努力工作以保证您的安全，依旧是件好事。然而，有些时候我们的直觉并不值得信赖，所以应该谨慎行事。

数字空间 —— 您的电脑、手机和其他电子设备，以及帮助它们通信的系统 —— 常常交织在您线下生活的整个结构中，但人们检测数字威胁的能力远不如检测物理威胁的能力更发达。

通过互联网和手机进行的监控和骚扰往往是非常隐秘的，很难察觉、难以防止或追究其责任。人们往往无法认识到这些威胁，或者反过来说，感觉到的威胁可能实际上并不存在。

为了更好地感知和计划应对这些威胁，必须更深入地了解我们日常使用的技术是如何运作的。

鉴于敏感人士正在遭受越来越复杂的电子监视手段，且不得不越来越多地依赖数字工具开展工作，需要认识到您的信息是一种宝贵的资产，并加深对信息的了解：信息是如何储存的，在哪里储存的，谁可以接触到信息。有了这些知识，您就可以采取行动，保护自己的信息和通信。

创伤、压力和疲劳

最后，创伤、压力和疲劳都会影响人的感知，从而影响人们识别和应对威胁的能力。

如果您经历了非常令人不安的或创伤性的事件，对危险迹象的反应就可能会被扭曲。一方面，这可能导致反应过度 —— 在不存在危险的地方看到危险；另一方面，创伤导致的精神疲惫可能意味着您会变得麻木，不再关注这些细节，无法识别真实存在的危险。

压力和疲劳也是如此，它们也会影响您现实地衡量环境中的威胁程度的能力。努力保持工作与生活的平衡，并对最近所承担的工作量和承诺的数量持现实态度，可以帮助您避免变得不知所措。

在日常生活中，一定程度的压力是正常的 —— 甚至是健康的 —— 它能使人们不至于变得无聊或沮丧。但是，即使您可以在短时间内应付较高的压力，但如果这种高水平的压力持续存在，人就会变得不知所措。这可能导致您的惊慌失措，最终沮丧，甚至可能抑郁。

这就是为什么您有必要学会如何调整自己。

[image]

因此，发展一种压力管理和自我照护的文化 —— 包括个人和团体、组织或运动，对于全面处理安全问题至关重要。这不仅有助于防止长期暴露在压力和疲劳中所带来的威胁，而且将大大有助于对安全问题的总体批判性思考。

从下面按钮进入本集内容的第二个和第三个练习，这些练习可以帮助反思我们的经验，包括过去如何看待和应对威胁，以及创伤性事件如何继续影响我们现在对危险的感知。更好地认识到这些问题，就更容易制定策略，使您的感知在未来得到"控制"，这也是您的安全计划和进程的一个关键组成部分。

[image]
[image]

“抓特务”不是解决方案：整体安全S01E02- 威胁响应

[image] 关键词	人际安全 团队 威胁响应 整体安全沟通
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月4日
[image] **Description**	教材

☝

酒肉朋友和患难之交的区别是什么？当您遭遇威胁时，您会期待谁与您并肩作战？…… 如果我们不能彼此照应，结果是什么？

您可以诚实地对自己说出加入这一组织/团队、参与这项工作的动机是什么吗？

- Table of Contents

  信仰和文化习俗是联结或分裂的根源
  威胁状况下团体会发生什么？
  1、变得更加封闭
  2、模式死板化
  3、变得更专制独断
  4、不信任和渗透
  就同伴和组织中的安全性进行沟通
  1、在团队中建立信任
  2、鼓励定期进行有关安全问题的讨论
  培养人际沟通的健康文化

1、围绕安全问题的普遍气氛是什么
2、意识到现有的等级制度
3、压力下的沟通
4、跨文化的情况
5、正式的沟通模式

圈子不是社区，两者有根本性区别。

在圈子里，人们的基本想法是 “你/你们能给我什么” —— 这可以是资讯、可以是人脉、可以是简单的被关注的存在感（挑起争论以获得聚焦）、甚至寻求新的约炮对象（性资本的炫耀/交易）；在这种环境下人们不得不拼命表现自己的“价值”，以避免被边缘化。

但在社区中，人们的基本想法是 “我们一起能做些什么”，“我如何能发挥自己的力量以协助我们的共同目标”。因为您不会担心被边缘、被排斥，每个人的力量和特长都能有用武之地，因为你们有一个共同目标，因此有足够的互信、协作以排除危险摆脱困境的动力。

在中国，我们听到过很多焦虑，基本都集中在缺乏信任以及竞争的压力方面，这是完全可以理解的 —— 当你们无法信任彼此时，就不得不隐瞒自己的信念；而当您被置于竞争环境下的时候，您将被迫更多地索取。我们对信任问题有过一些解释，也对渗透的操作给出过具体分析；在我们看来，人们唯一缺乏的是一个共同目标，目标就是信任的指标，也是将竞争良性化以提高效率的最佳工具 —— 想想看，如果您发现其他人的努力朝着你们的共同目标坚定地前进，您甚至不需要知道对方的真实名字，也能将其视为联合力量，对吗？另一方面，只有在个人利益高于共同目标的情况下，人们才会因竞争而互相排挤。

但是，并非建立一个共同目标就能化解一切问题，组织和沟通技巧仍然非常重要（本项目将单独开设相关战术话题的站点），而且需要您的实际练习才有希望实现它。这就是本教程的主题。本教程需要系统化的掌握，单独任何一篇文章可能都无法真正帮您解决问题。

[image]

欢迎来到第二集。

敏感人士对于自己的工作的看法和自己的安全概念，在一定程度上都是内心信仰和价值观的产物。是您的身份意识和对世界的看法推动和指导着您的行动主义，并支持您如何开展工作。它也是您处理安全问题的方法。

内心的信念和价值观可以成为帮助您保持专注、保持安全和建立复原力的宝贵资产，无论这些价值观是宗教的还是精神的，是无神论的，还是基于家庭或社区的。

信念往往非常个人化，有些时候您可能不会在小组成员和同事面前提及它，您担心无人理解；但是在很多情况下，正是这些信念而不是那些高大上的口号，共同推动着人们完成任务。

喊口号很容易，但如果人们对口号无感，您就无法真的凝聚人们。

所以，不要羞于谈论您最真实的内心信念，您的动力之源。只有这样才能让您和您的队友产生真实的连接。你们之间的连接是否真实，是你们能否抵御侵害的基础。

创造一个安全的共享空间来开放您自己的内心是很重要的。理想的情况是，您可以在这样的环境中取得成就：您的个人信念会得到尊重，也建议您对其他人的灵感和复原力来源表示同样的尊重和鼓励，如果他们与您不同的话。

对您的信仰采取集体开放的态度，可以培养一种尊重、理解的文化，使同事之间的工作关系更加密切，并能缓解分歧、紧张和不信任。

人们很容易认为，因为您和您的团队或同事都在为一个共同的目标而努力，所以你们的信念是相同的。事实不一定如此，如果您能花时间去了解和理解对方的个人信仰，就能更好地理解对方。

为了创造一个健康的工作环境，敏感人士的工作空间必须是开放和尊

重的，每个人都感到能够分享激励他们的价值观，这种方式不会导致评判、争论或教条，而是促进团结、相互尊重和学习。

在对安全问题采取全面做法的背景下，敏感人士应当明确为这种分享提供空间，以便承认激励不同的价值观，帮助你们建立复原力，并在危险面前继续工作。

[image]

信仰和文化习俗是联结或分裂的根源

尽管信仰和文化习俗可以成为一个团队内部的团结或联系的主要因素，但它们也可能成为相反的因素 —— 如果您作为组织者不鼓励少数群体的做法，它们就会成为一种分裂的力量。这不仅会对那些被边缘化的人产生负面影响，而且会对整个群体产生负面影响。

从更广泛的社会来看，信仰和文化习俗可以在你和你想改变的社会之间形成一种统一的（也许在战略上有用的）联系。然而，它也可能成为一个分裂因素，将你与“他人”分开，并可能被利用来羞辱或针对你。

这一问题将在本教程的后面部分将做更多具体介绍。

敏感人士很少会独自一人工作，也很难做到独自一人：在制定全面的安全办法时，认识到您的团体、组织和社区如何集体应对威胁，以及团体动态如何在危险面前发生变化，是很有帮助的。这将有助于您确定群体动态的困难方面和改善沟通的战略，以建立团结、信任和更好的安全做法。

威胁状况下团体会发生什么？

与个人一样，当部分或所有成员发现自己受到威胁、被边缘化或被暴力（包括经济、性别、体制或结构性暴力）时，群体动态也会发生变化。

群体动态变化的具体方式在很大程度上取决于相关群体本身。

一些可预测的群体反应包括以下内容：

1、变得更加封闭

该团体开始加固其围栏，使成员更难以离开、同时其他人也更难以加入。这种封闭也会限制成员获取信息的机会，或减少他们将自己对事件的看法与外部各方的看法进行比较的机会。简单说，变得更加井底之蛙。

您知道中国异议人士的小圈子吗？嗯，就是那样。这与不擅长组织动员有一定关系，但更多的原因是被当权者的渗透和镇压吓到了。

这也正是镇压者最希望看到的状况：自闭的、极化的、虚无主义盛行，无法再联合起来利用自身庞大的基数给统治者带来压力。

2、模式死板化

第二个可预见的变化是，敏感人士群体的行为模式会变得更加固定、死板，更难改变。因此，成员们更难对现状提出质疑。

这也是为什么新颖的反抗模式和安防措施非常难以接触到某些长期工作的敏感人士，似乎越是“资深”就越是自闭和顽固。您也许可以理解这点，因为对于这些敏感人士来说，他们感觉到的是“我好不容易找到了一个合适的模式，对它的任何更新都可能是危险的”。

✂

良好的组织是，各团体必须定期以诚实的方式重新审视和讨论其共同的价值观，以保持公平和包容性。

3、变得更专制独断

第三个可预测的变化与群体内的领导和权力动态有关。当群体感到不安全时，成员就会倾向于容忍领导者或群体中其他更有权势的成员的更大的专制行为。

在极端的情况下，群体中的强势成员可能会滥用权力，而群体边界的日益僵化可能会阻止受害者离开。

这也是一种棘轮效应 —— 面对灾难和威胁的人们倾向于寻求更强大的权力的保护。

这种情况非常常见。您一定记得异议人士群体内为什么普遍表现偏执，大多数理性思考都恐怕被怀疑为“立场不坚定”，从而被边缘化。这样一来反抗群体将更加难以获得进步，参与者变得压抑呆板，失去了创造力。

从决策与安全之间的联系来看，我们不应低估公平和透明的决策过程的积极影响。如果一个团体能够具备共同的责任和知识，那么你们的对手针对你们的威胁就不会那么明显。

也许您可以在您自己所在的圈子/群组中识别出其中的一些行为，也或许您发现了更多不同的现象。不管怎样，在任何情况下反思您的群组在受到威胁时经历的任何变化都是非常好的做法 —— 请记住，不同人对这一点的看法可能有很大的不同 —— 并找出你们也许可以改进的任何共同问题。

保持开放的对话和沟通渠道将提高你们避免这些和其他破坏性行为的机会。后面将更详细地介绍如何培养健康的安全沟通文化。

[image]

4、不信任和渗透

不幸的是，渗透是常态，是全世界任何活动团体或组织面对的共同问题。（本站有专门栏目讲解防御渗透的方法）

对渗透的了解往往会带来更多的互不信任和危险意识。同时，压力和创伤也会增加敏感人士之间的不信任感。

敏感人士必须考虑到自己的团体或社区的一些成员会否成为告密者的可能性。请注意，妖魔化任何人都是无济于事的；在压迫的背景下，他们往往也是受害者。

在这种情况下，您最好的选择采取措施来保证社区的整体安全，而不是助长怀疑和不信任的气氛，因为这可能会导致“猎巫”，对您自己和您的事业都产生负面影响。

建立公开的小组讨论，就如何处理敏感信息的透明程序达成一致，以及定期审核关于保密和小组活动透明度的决定，都会有所帮助。

渗透者和政府线人往往试图记录甚至鼓动敏感人士团体采取无意义的暴力活动。请在您的培训项目中加入这里所论述的原则，以增强队友们的判断力。

对于那些鼓吹恶毒的或暴力手段的成员，应小心处理，并检讨其成员资格。

就同伴和组织中的安全性进行沟通

如上所述，一旦敏感人士能够更好地了解个人和团队对压力和威胁的

反应，就可以在自己的团体和组织中引入健康的做法，以防止或应对你们发现的任何共同问题。

然而，可能依然会有一些障碍阻止您在组织内公开讨论安全问题，例如 —— 沉重的工作负担、恐惧、担心自己的观察会被误解为偏执狂、性别问题和权力动态等。

您应该努力建立信任的氛围，安排有关安全的定期检查，以及建立健康的人际沟通文化，这将帮助您：

- 更准确地感知威胁
- 了解团队成员为什么会对压力或威胁做出不同的反应
- 更准确分配安全措施的角色和责任
- 增加团队对安全措施的掌握能力
- 团结和关怀遭受威胁的同事

下面将详细探讨这些策略中的每一种。

1、在团队中建立信任

只有在您真的信任与您一起工作的人时，才会更容易实施安全措施，并且彼此间更容易分享担忧、经验、甚至曾经错误的教训。

建立信任的方法有很多，不同的组织也会有所不同。您可能想从工作之外的相互了解开始，定期检查团队的健康状况、压力水平、以及团队成员的个人生活是否影响到工作（反之亦然）。

围绕决策结构的透明度，以及如何处理个人或敏感问题的明确协议，也是一个好主意，如果能有一个值得信赖的顾问或心理学家那就更好了。跨领域合作非常重要。

在团队中建立信任并不是一件容易事 —— 考虑到前面提到的渗透的广泛可能性，它涉及赌注和承担风险，但它同时也可以激励您建立、并信任您和队友们管理敏感信息的策略。

信任的氛围还有赖于每个人都能给予和接受建设性的批评和反馈，这将在下文中进行更多探讨。

2、鼓励定期进行有关安全问题的讨论

必须创造定期的、安全的空间来讨论安全问题的不同方面。您和队友之间必需能互相知道对方的发现和经历。

这将有助于敏感人士团队将安全视为一个重要且有效的议题，并使您在提出关切时感到更加自在。如果您的团队已经定期举行小组会议，就可以利用这些会议来分享安全局势的任何潜在变化（后面的内容将更详细地探讨这点）。

在为每个项目或活动进行战略规划和准备时，也应留出空间考虑安全问题。这样一来，安全问题就可以成为团队成员经常思考的问题 —— 成为行动主义的一个组成部分，而不是一个单独的话题让别人去担心。

在高风险的情况下，增加检查次数，鼓励成员讨论安全问题是非常必要的。

从这里进入本集的第一个练习，帮助您思考如何以及何时与同伴、同事或团队谈论安全问题。

培养人际沟通的健康文化

即使敏感人士认识到了谈论安全的重要性，也会感到困难。安全是一个非常个人化的话题，在讨论自己的弱点时，不管是什么弱点，人们都很可能有一种被暴露的恐慌感。

作为组织者，您需要确保人们感到交流的安全和尊重，并避免误解或冲突。以下是需要考虑的一些因素，这些因素可能会影响到团体和组织中关于安全的交流。

1、围绕安全问题的普遍气氛是什么

围绕安全的现有(组织)心态是什么？分配给讨论安全问题的时间是否与其他会议时间一样受到重视？当讨论安全问题时，小组成员的声音或语气是否不屑一顾？当您的同事在讨论他们的关切时，您是否真正感兴趣并与他们建立了个人联系？

如上所述，创造明确的空间来解决组织的安全问题是有效安全规划的基本步骤。

2、意识到现有的等级制度

平等。平等在这里不是口号，而是一个重要的交流条件 —— 在您的组织内建立跨等级的沟通机制，以便成员能够在没有权力关系压力的气氛中讨论问题。

3、压力下的沟通

在压力增大的时候，注意您在团队中的沟通方式变得尤为重要。当遇到威胁或压力时，人们可能不会总是以尊重的方式进行沟通。

4、跨文化的情况

还必须记得，沟通是文化和文化多样性的一个基本方面。您应注意在跨文化情况下的语言和非语言交流。

5、正式的沟通模式

一些团体和组织在沟通和会议决策方面往往比较正式。如果每个人都在正式场合共同讨论并做出决定，那么关于安全的决定往往更有可能得到支持。

然而，这种沟通模式有时也会限制分享安全问题的更多情感方面的内容：在这方面，可能值得考虑其他的促进方式，为这种分享创造空间。

在敏感人士的一般工作中，但特别是在试图围绕安全问题促进公开和健康的沟通时，“非暴力沟通技巧”可能非常有用。

非暴力沟通是一种基于以下假设的沟通方法，即：所有人都有同情心，我们都有同样的基本需求，我们的每一项行动都是满足其中一项或多项需求的战略。

采用这种方法，它可以成为促进健康的跨文化交流的有效途径，特别是用于提供和接收有关安全的反馈，以及讨论攻击、事故、威胁或其他与安全有关的事件对我们个人和团体的影响。

您可以通过本集的第二个练习来了解更多关于非暴力沟通的知识。

[image]
[image]

知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者

[image] 关键词	团队 威胁识别 战略图谱
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月5日
[image] **Description**	教材

确立您的目标，分析您身边的所有人 ……

- Table of Contents

  不断变化的威胁
  将遵循的步骤
  分析与感知
  愿景，战略和参与者
  建立您的愿景和行动
  扩大认识
  映射角色之间的关系
  最后

[image]

欢迎来到第三集。

在前两集中我们介绍了整体安全的基本概念和须知，并针对敏感人士

最常见的危险 - 如 渗透和内部分裂 - 提出了一些想法；建议您按顺序阅读本系列，其中的练习题都很重要，因为这是一个解决方案的框架，只有通过实际练习，才能真正解决您自己的组织中面对的具体难题。

建议敏感人士对自己所处的环境进行系统性的分析，这是一项很重要的活动，它是能力的基础 —— 帮助您设计和维持最新的和准确的安全战略。随着您的生活和工作环境的变化，您的安全状况也自然会发生变化。

不断变化的威胁

您面临的威胁在不断变化中，只有承认这一事实并作出相应的计划，安全战略才会有效。这就是为什么无法有一套通用的、甚至持续有效的安全措施，寻求固定不变的安全建议或者任何人承诺存在这样的安全建议，都是不现实的。

如果只是习惯性地或根据听来的说法采取防御，您很可能会发现它们不够实用，尤其是不断变化的环境使这些措施失去效力。

本集内容将概述敏感人士可以如何提高对不断变化的环境的认识，制定战略以实现您的目标，同时避免、减少和减轻可能出现的威胁的不同方法。

这些步骤中的许多您可能已经熟悉了，也可能已经在实践：但是，如果可能的话，系统化地进行这些步骤是非常有帮助的。在后面的内容中，我们将按照从一般到具体的顺序，深入探讨每一个步骤。

当然，在实践中使用这些工具的顺序取决于您自己和您的组织的具体工作和规划过程。

本系列内容全部都在强调框架性 —— 您需要基于此框架并根据您的

具体情况，设置最适合的方案。

将遵循的步骤

1、情况监测和分析：

观察与您的工作有关的总体趋势 —— 政治、经济、社会、技术、法律或环境，并注意与您的安全有关的任何事态发展。

这是新闻能给您带来的最好的东西。您需要做的是，有目的地阅读新闻，在这里，您的目的就是安全措施更新；当您具有一个实际性的目的（而不是为了吐槽时），您将会从那些平时看起来普通的消息中发现有价值的细节。

社交媒体总是鼓励人们吃瓜吐槽，它以影响力提升来奖励吐槽，从而压制重要的思考和行动。摆脱它。粉丝量除了虚荣的面子之外毫无价值，社交媒体灌输给人们这个价值观只是为了帮助那些巨头公司赚钱；尤其是对于那些并没有打算利用粉丝做生意的真正的敏感人士来说，摆脱这种错误的价值观才能帮助您找到真正有意义的社交媒体使用方式。

2、确立您的愿景和活动：

在上述基础上，您可以反思自己所发现的问题、所设想的社会变革，以及您用什么策略来实现这种变革。

当您的目标确立时，这一切价值都将自然而然地出现。

3、行动者和关系图谱：

建立和维护一份将受到或可能受到您行动影响的所有人员、团体和机构的清单，包括您自己、您的盟友、和您的反对者。这将有助于为您的宣传战略提供信息，以维持您的工作空间。

简单说，您需要知道自己面对的是什么样的人，哪些人值得合作、以什么样的方式合作，哪些人需要提防，他们有可能对您构成什么样的危险和阻碍。

让您的行动计划更有效力。

4、信息图谱：考虑您的个人和职业信息，并确保这些信息不会丢失、损坏或落入坏人手中。

请注意，您的任何信息都可能为攻击者提供捷径，但没有哪一种信息可以成为直达的捷径 —— 它们往往被组合起来使用；所以，您不必担心难以保护所有信息，您只需要做到被暴露的信息真假交杂、并尽可能少地暴露，效果就会更好。

5、安全指标：

注意到不寻常的事件，这些事件可能表明您的安全状况发生了变化。随着时间的推移，分析其中任何可能影响您的安全战略的趋势。

也就是态势感知。不论是在线还是现实，这一点都非常重要 —— 如果我们能在2003年就了解到KIS（Knowlesys Intelligence System），也许那之后不会有如此多人因推特和Facebook言论而被捕。

当下最重要的问题是，他人/其他社区对态势变化的了解应该能惠及所有需要相关信息的社区和敏感人士个人；它需要能够为策略调整提供重要的参考，而不是局限在点评上。做到这点需要您具备清晰的目标和敏锐的感知力，如果您无法摆脱社交媒体，也需要意识到算法操纵和 “影子禁令” 如何对内容进行限制，并有意识地通过搜索策略来避免错过重要信息。

6、威胁识别和分析：

在进行了上述所有工作后，识别出您认为可能发生的或有潜在危害的

事件或他人的行为，并做好准备。分析这些威胁的背后是谁、有哪些资源可以降低其概率或影响，以及接下来要采取哪些步骤。

7、安全规划和战术：

在以上分析的基础上，您可以确定并采取具体的措施来改善您的安全状况了。对于这一步骤后面文章中将有更详细的探讨。

所有这些工具都可以根据您自己的计划过程进行迭代使用，以保持其及时的更新。这一点很重要。

[image]

分析与感知

上述进程旨在帮助您尽可能客观或科学地判断您的安全局势。然而，安全问题从根本上说仍然是一个人的认识问题。

在第一集中我们已经详细介绍了人们对安全的 “主观” 体验所带来的挑战和机遇 —— 您对威胁的认识可能受到挑战、受到限制或存在缺陷。可能存在您没有能识别的威胁 —— 由于环境不熟悉或由于您的对手（尤其是当权者）成功地隐瞒了这些威胁，如电子监控，导致您无法识别；或者是没有根据的恐惧 —— 对您没有实际危险的事，但由于您的对手太过强大或您自己的焦虑情绪反应（可能与过去的创伤经历有关）所引发的错误信息，依然将其认定为威胁。这部分内容将在后面文章中作出更多具体分析。

这个问题很重要，敏感群体容易爆发类似 “受迫害妄想”，并同时又会因过度恐惧而导致消极的虚无 —— 认为自己做什么都是 “无意义的”，为了缓解紧张情绪宁可相信 “没什么可隐藏的” 。这反而给了您的对手以可乘之机.

如果您能考虑到所有这些因素，就更容易对您所面临的威胁程度有一

个现实的认识，尽管这仍然具有挑战性。面临的挑战是减少未认识到的威胁和毫无根据的恐惧的数量，以便您的安全做法尽可能有效。

您可以通过进行研究和分析，以及与值得信赖的朋友或同事核对你们的共同认知，来提高您的认知的准确性。

愿景，战略和参与者

只要是对社会上的问题和国际上的事态发展有所了解的人，都不难发现人权方面存在的问题、不合理和不公正现象。其中作为反抗者的人们，需要通过这些了解来明确我们的变革愿景 - 我们想要的世界是什么样的？

对许多反抗者来说这一点已经很清楚，但有时人们没有花时间清晰阐明和界定自己的愿景或目标。

意识到这一过程有助于制定战略，而战略又能指导您就安全问题作出决定。

路径：您的愿景和目标是什么，以及您如何着手实现这些愿景和目标，这将决定社会上哪些其他行为者将采取行动帮助或阻碍您的工作，从而影响您的安全状况。

在团队中工作时，对您的战略进行批判性思考就变得更加重要了。对您要实现的变革和如何实现变革，保持透明和公开，不仅可以防止您的组织内部的隔膜和冲突，还可以防止您的社区或整个社会的困难和冲突。

[image]

建立您的愿景和行动

为了帮助建立或刷新您对变革的愿景，请问自己以下问题：

- 您希望解决的问题是什么？
- 您希望看到什么样的变化？
- 如果实现这一变化，之后您的社区会有什么不同？
- 如果您成功了，人与人之间的关系会有什么不同？
- 涉及此问题的其他个人，团体，机构等是谁？他们对您的行动有何反应？—— 是与您合作、还是拼命阻止您？

当您对自己想要实现的目标有了清晰的认识时，就可以开始思考 “如何” 做到了。您应该实施哪些方法和行动来实现您的目标？哪些是您已经在做的？还可以做些什么？哪些活动在实现您的目标方面可能并不像您之前所想的那样有效？ 如果有必要，可以在您的团队中抽出时间来批判性地思考这些问题。

您开展的活动、以及您在开展这些活动时的行为，决定了国家、社会和您周围其他人对您的看法。您如何与这些行为者 “互动”，将决定他们对您的反应 —— 影响他们容忍、接受或拒绝您的工作并试图封锁您的工作空间的程度。

因此，清楚地了解您所处的环境中的所有行为者（个人、机构、组织等）是很有价值的。威胁几乎总是来自某个人或某件事。尽可能多地了解您所处环境中的行为者，可以提高您对环境的认识，从而提高您开展活动以维持或扩大工作空间的能力。

其中一些行为者可以被视为朋友或盟友，另一些行为者则是对手，还有一些行为者则处于中间位置，是中立的一方。📌 每个人都有自己的利益和资源，有可能帮助也有可能阻碍您的工作。

了解这些行为者是谁以及他们的行为如何影响您，将使您的安全计划受益。通过完成本集第一个练习，以绘制您自己领域中的行为者、及其与您的关系的性质。

[image]

扩大认识

您可以将这些行为者分类3类：

1、盟友 —— 与您的目标在战略上保持一致的人，尽管他们的支持力度和持续时长可能会随着时间而改变。

2、敌手或对手 —— 其战略利益与您的利益相反的那些人，包括出于各种原因以某种方式反对您的目标的人。同样，请记住，反对或对抗的强度可能随着情况的变化而变化。

3、中立方 —— 这些行为者既不支持也不反对您的事业；但是，他们的作用可能会随着形势的变化而改变。

将这些参与者想象成一个图谱可能会很有用。

这种 “盟友图谱” 经常被用于设计运动作为战略设计的重要部分之一，以确定您想要影响的人。您也可以利用这个范围来进行安全规划，并促进国家和社会不同阶层对您的工作的认可，即：有计划地通过不同的倡议活动和参与协调。

为了确定优先次序，您可以首先关注您所处环境中活跃的盟友和对手，并更深入地挖掘他们的动机和资源。这对于分析潜在的（或实际的）威胁、以及谁在积极或无意中操控这些威胁的关键步骤来说是很有用。然后，在绘制您周围的行为者之间的关系图时，您可能会看到可以用来改善您与对手关系的途径（例如，通过相互接触）。

映射角色之间的关系

下一步就是分析、确定、和具体说明行为者之间关系的性质。这对于确定其动机可能导致威胁到您或您的工作的行为者、以及可以依赖以帮助您更安全地工作的盟友，特别有用。

要做到这一点，请尝试以下练习。

最后

您可以将行为者图谱存储在可以定期查看和更新的地方：虽然一开始您可能会以可视化方式进行操作，但随后您可以创建一个文档，如 电子表格，您可以在其中保持关于图谱中确定的关键行为者的最新信息。

在考虑您的安全策略和新出现的威胁时，这样做是很有用的。

在对您的社会政治环境有了很好的了解之后，现在就应该开始考虑到您的数据和信息对您的工作和安全意味着什么了。

下一集我们将进入这个重要步骤。

[image]
[image]

夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产

[image] 关键词	信息资产
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月6日
[image] **Description**	教材

敏感人士的信息安全性至关重要，事关本人和相关一群人的生命安危。因此如何保护信息的问题可能会引起焦虑。有效且及时更新的信息安全策略可使您放心地专注于自己的反抗目标、并以健康的方式开展工作。

- Table of Contents

  常见威胁
  信息类别
  静态信息 ——
  动态信息 ——
  数字形式的信息
  通过数字渠道了解动态的信息
  映射您的信息生态系统
  1、这是什么信息？

2、它在哪？
3、谁有权使用它？
4、它有多敏感？
最后

恐惧来自未知。

人们只会害怕那些自己没有充分了解的东西，黑暗和模糊会产生可怕的联想。

很多时候敏感人士看到的往往只是抓捕、迫害、骚扰、各种惩罚手段，人们被吓坏了，开始认为“对手无比强大”，甚至“不论如何我都无法逃脱”。这并无助于解决问题，相反，却给了您的对手一个肆意妄为的机会。

未知带来的恐惧会让您陷入困境。

本教程希望引导您和您的组织通过分析拨开迷雾，点亮那些黑暗的角落。当您对自己和对手有了一个全面了解的时候，您才有希望进入精力充沛的对战状态。

[image]

欢迎来到第四集。

敏感人士如果想要全面了解自己的安全状况，就必须将您的信息作为您在工作中产生的和使用的重要资产，并仔细研究它们与您的安全之间的各种关系。

本集内容将鼓励您系统性地绘制信息概况，并探索对其完整性的威胁，从而得出保护它的最佳方法。

首先需要了解的是，当在工作中谈论“信息”或“数据”时，它指的是许多东西，例如：

- 您工作的产物；报告、数据库、图像、语音和视频记录；

- 运营信息；例如您的短信、文件和进度报告以及其他办公信息和通讯；

- 可以将您识别为某个组织成员或专业联盟成员的个人信息；

- 您在工作时通过使用数字设备生成的数据 即“元数据”，可用于跟踪您的活动或监视您的私人关系。

这些信息可以以多种方式储存和传播，一旦被恶意者获取，就会让您的对手对您的行动和团队关系有一个令人震惊的全面了解。

这就是为什么它必须是非常宝贵的资产，必需谨慎对待。随着敏感人士越来越多地接触数字技术，特别是近年来，您的对手对进入您的设备或截获您的数字通信越来越感兴趣。

不幸的是，敏感人士得到的帮助经常是错误的和过时的，大多数最流行的数字工具几乎不能保护您的信息免受资源充足的对手的攻击 —— 比如政府和间谍。并且，您需要知道，您的一些对手很可能与提供您的软件或在线服务的公司或机构有着秘密且密切的合作关系 —— 请思考斯诺登文件，以及您在中国了解到的同类事；因此，将这些供应商也添加到您的行为者图谱中是很必要的。

因此，敏感人士尤其应该学习一些数字技术的基本运作方式，提高自己的数字素养，这是您的行动主义中重要的且有力的一步。

[image]

常见威胁

1、数据丢失 —— 由于计算机卫生状况不佳、恶意软件感染、断电或

硬件老化，计算机和其他设备有时会停止工作，从而导致丢失数据。

2、账户入侵 —— 有时，您的密码或“秘语”并不是很难破解，或者您遭受到网络钓鱼攻击（可能是随机的或特别针对您的），并在不知情的情况下将凭据泄漏给了第三方，继而被攻击者访问您的电子邮件或社交媒体帐户。

3、设备被警察没收或被盗 —— 电子设备是小偷最看重的目标，因为这里面远不止物件本身的价值。在威权国家生活的人，比如中国人，尤其需要注意的是警察和国安部门强行拿走你的电子设备。应对这点的方案见下一个教程**S02**。

此外，如果您的工作面临严峻的风险，您的办公室和住所可能会遭到国家或非国家行为者的袭击，计算机、手机、硬盘驱动器、USB密钥和服务器，都可能会被“没收”或被盗，以进行所谓的数字取证。

4、强行搜查 —— 中国人对于查手机应该再熟悉不过了，这在其他国家也是如此，尤其是过境点，比如美国。敏感人士可能会在通过边境或军事检查站时被暂时没收电子设备，这一过程中可能会复制您的数据、甚至有更糟的可能，比如被感染间谍软件或连接了硬件键盘记录程序。

5、信息被移交 —— 如果警察能拿到传票，互联网服务提供商以及您使用的电子邮件和社交网站的提供商，就必须将您的数据移交给某些政府机构。这种情况正在根据商业利益和政治利益而不断变化，随时都会发生。

6、追踪监视 —— 数据经纪人、互联网服务提供商、电子邮件提供商、和许多其他公司，一直在通过收集和汇总您的在线活动的详细信息，对普通人群进行监视和操纵。这就是监视资本主义。

它将所有人变成深入的监视目标，当然也包括敏感人士。

7、被恶意软件瞄准 —— 有针对性的恶意软件是一个正在快速发展的行业：一些国家机构和其他组织花了很多钱投资那些旨在诱使敏感人

士下载并随后允许攻击者访问其设备上的大部分或全部数据的软件。

并且，这些武器级的间谍软件一直在基本不受阻碍地出口。

敏感人士信息的安全至关重要，事关本人和相关一群人的生命安危；因此如何保护信息的问题可能会引起焦虑。有效且及时更新的信息安全策略可使您放心地专注于自己的反抗目标、并以健康的方式开展工作。

要做到这一点，第一步就是要对您的信息的所有实例或版本进行尽可能编目。

对您自己的信息 “生态系统” 中存在的元素有一种心理上的理解，将有助于摆脱将 “信息” 视为模糊的海量数据的认识，而将其更好地理解为有形且重要的资产。

通过将您的信息分类为各种组成部分和类型，您可以确定自己的信息可能或不可能变得脆弱的任何潜在情况和途径，以及需要改进其安全性的领域。

此过程取决于上一集附带的练习的结果，在此过程中，您已经确定了背景中的 “参与者”，包括您自己、盟友、反对者、和当前的中立方。您可能会回溯并扩大参与者图谱，以通过信息映射过程确定潜在的新参与者。

这就是为什么要建议您按照顺序阅读本教程，因为内容是进阶的。

该图谱还将有助于理解您的信息要素与您的盟友和对手及其意图和能力之间的关系。

接下来将介绍一些关键概念，以了解如何对您的信息进行分类，然后进行 “信息生态系统” 练习，这将有助于您绘制最重要的信息资产的图表。

[image]

信息类别

制定信息安全策略的第一步是了解您所拥有的全部信息、这些信息所在的位置、以及如何从一个地方转移到另一个地方。

开始此分类过程的一种简单方法是根据动态的和不动的状况来思考。例如，存储在文件柜中的财务信息 —— 静止不动的信息），在即将发生的事件中通过移动电话交换的消息 —— 动态的信息。

这种区别主要用作组织原则，以帮助进行分类。重要的是要记住，当今您的许多信息都是数字形式的，并且随着互联网和远程存储服务（即所谓的 “云”）的使用不断增加，您拥有的许多信息都在运动中。

同样，由于手持设备（例如智能手机和平板电脑）的日益普及，存储容量的增加以及这些设备的实际移动性，存储在此类设备上的任何信息（尽管可能是数字“静止”的）实际上都是在物理空间中移动。

值得重复的是，在以上分类中，您的通信（例如电子邮件、聊天、短信、和电话）是 “运动中的信息”，并且这是非常普遍的，尤其是在通过互联网保持近乎恒定的连接的情况下。

当您决定采用策略以更好地保护自己的信息时，这种组织原则就很有用，因为有多种方法可以保护静态信息和动态信息。

静态信息 ——

一旦确立了愿景，您就必须考虑可以采用什么样的方法来实现它。

您可能会以个人或组织的身份开展各种各样的活动，以实现反抗目标。您的 “工作领域” 或从事的活动是什么？重要的是要明确列出它

们，并首先考虑它们是否适合实现您设定的目标。

您的工作不是在真空中进行的，而是在丰富多样的环境中，通常会具有一些冲突的特征。您的行动策划是您与这些冲突以及您试图影响的国家和社会的“接口”；是您试图改变周围环境中各种行为者（个人、机构和组织）的状况、看法和行为的手段。其中一些参与者将从中受益，相信并支持您的行动；但是其他人会觉得这些行动不符合他们的利益，并会试图缩小和压制您的工作空间。

所有这些通常都可以提供有关个人、项目、运动或组织的信息源，因此，盗窃和没收计算机、手机和存储设备是镇压敏感人士的常见策略。

在整理您的“静态信息”列表时，请考虑下面这些问题：

- 这些信息在哪儿？
- 谁有权访问这些信息？
- 这些信息的内容对您、您的组织或文档中提及的任何人员 —— 例如目击证人或受害人 —— 有多敏感？
- 保留这些信息有多重要？
- 应该保留多长时间？

动态信息 ——

如前所述，您拥有的许多信息资产 —— 尤其是数字形式的信息资产 —— 在某个时候从一个地方传输到另一个地方。请考虑您的信息移动的所有方式：

- 装满文件的盒子，通过快递投送

- 通过移动网络拨打的任何电话

- 在线上传到某个服务器的任何视频

- 参加抗议活动时手机中的任何联系人信息

如上，您可以看到信息移动的各种方式：在物理空间中传播的物理信息，或在互联网上传输的数字信息，或在物理空间中移动的数字信息（存储在物理设备中的数字信息）。

还应该注意信息移动的不同方式：

1、传输：无论是在办公室工作期间，还是通过互联网将附件发送给同事，或者将敏感文件备份到另一位置的服务器时，您的信息都从一个点传输到另一个点。

2、交流：当您与同事、盟友、公众甚至反对者互动时，就会发生信息交换。通信可以采取以下形式：在事件发生时从扬声器宣布指令，或者在电话交谈、视频通话、面对面的会议、电子邮件、短信等途径交换机密信息。

您的交流中包含许多有关您的意图、您的行动状态、您的计划和未来活动的信息。

要对此类信息进行分类，除了上述 “静态信息” 中提到的属性外，您还可以考虑以下内容：

- 信息如何传输？

- 采取的是哪种物理或虚拟路线？

- 谁可能在信息传输途中访问它，或者谁会对捕获它感兴趣？（考虑您在前文的练习中构建的行为者图谱）

[image]

数字形式的信息

与数字形式的信息相关的一些独特属性值得考虑：

1、复制：不断复制数字形式的信息。在文件传输、电子邮件交换、上传和下载期间，甚至当从一台设备移动到另一台设备时，都会创建信息的副本，这些副本的所有意图和目的都与原本相同。

这与前数字时代稍有不同，前数字时代有可能（尽管有时困难）区分原始信息和随后的副本（例如，在纸上直接打字的会议记录）。

2、信息的“永久性”：如上所述，一旦将一条信息上传到互联网，上传、传输和下载的过程中就需要多次复制此信息。因此，您的信息可能会遍历您无法控制的互联网部分而保留在某处。

当邮件服务器、路由器和其他中介复制信息以帮助传输过程或出于其他目的（取决于控制设备的人的意图）时，就会发生复制和中继。因此，重要的是要理解，信息传输中的一个（或多个）参与者将在很长时间内保留某条信息的副本，不论是有意的还是无意的。

例如一条短信，它是从一个手机发送到另一部手机的，但是在发送过程时，它会通过多个蜂窝塔和属于服务提供商的其他基础设施。服务提供商可以访问这些消息，并且在大多数情况下，无论您是否从自己的手机中删除它们，它们都会保留很长一段时间。

3、元数据：随着计算机和数字设备执行其操作，会创建一层“元数据”。此信息随数据本身一起提供，有时无法将其从数据中删除。

元数据的示例包括：

- 您的IP地址（用于确定您要连接到互联网的位置）以及您访问的网站的IP地址。
- 移动电话从一个点移动到另一点时的位置数据，即SIM卡和手机的唯一标识符（IMEI码）。通常无法更改手机的IMEI。
- 电子邮件的发件人、收件人、时间戳和主题，以及它们是否包含附件。由于服务器需要知道向谁发送电子邮件及其附件，因此无法删除此信息。但是，其中一些可以更改或模糊化。
- 图像文件的属性，即 有关照片拍摄位置、大小和用于产生图像的设备的信息（相机和镜头的品牌、用于编辑图像的软件等），某些信息可以使用图像处理软件删除。
- 文档的属性，即 有关作者的信息、文档的创建或修改日期等。可以通过更改文字或电子表格处理者的个人隐私设置、或使用元数据剥离软件（例如元数据匿名化工具包）来删除某些此类信息。

元数据经常被忽略，因为它不是您自己创建的，甚至可能没有意识到的。但是，在考虑您的信息生态系统的不同元素时，应该牢记它的存在并采取适当的步骤来了解其范围和可能产生的后果。

可在本站的“工具”板块中查找元数据工具。

[image]

通过数字渠道了解动态的信息

当考虑通过数字渠道传播的信息时，上述属性起着重要作用，因为信息可以很容易地复制和存储。

通过数字渠道传播的信息几乎总是在物理空间中移动，例如从您的手机开始的状态更新将进入社交媒体网站，该网站实际存储在特定位置的服务器上。甚至一路上可能会经过许多不同的国家。为了考虑可以确保信息安全的方式，就必需考虑信息的来源、目的地以及信息的路径。

[image]

虽然您可能知道信息的来源 —— 例如在笔记本电脑上键入的电子邮件，但还需要注意信息的目的地 —— 例如，通过其邮件提供商的您的同事/朋友的收件箱，以及沿途的所有站点， 包括：

- 互联网服务提供商
- 运营互联网基础设施并传输您的数据的电信公司
- 在数据和元数据通过互联网传输时进行主动捕获和监视的国家实体
- 对这些站点和网络服务具有控制权的任何其他实体，是否可能对捕获数据感兴趣
- 其他第三方（例如广告公司）可能会收集有关您在线活动的任何数据

花点时间学习或复习互联网和移动通信工作原理的基础知识，有助于阐明这一过程。 这样做可以减少因被监视而导致的焦虑或毫无根据的恐惧 。

还应考虑包括用于保护数据的加密类型（如果有的话）。加密是为减少可以访问某些信息的人数的技术手段。它通常由服务提供商（例如银行网站或某些通讯应用程序）提供；您也很有必要学会使用特定软件对您的信息或通讯进行加密（在本站“工具”板块中查找），以确保不会被未知的人访问。

您可以据此分析在您的行为者图谱中添加一些内容。您可能会发现自己需要调查这些行为者与您的盟友或对手之间是否存在任何关系。返回行为者图谱，令其包含以下内容：

- 您的互联网或网站服务提供商

- 您的电话服务提供商

- 您的电子邮件和社交网络服务的提供商

- 与上述内容有关系的任何相关实体（例如政府机构）

在下一部分中，您将通过练习映射 “静态” 信息和 “动态” 信息，这将帮助您确定信息管理实践中的差距以及弥合这些差距的方法。

映射您的信息生态系统

如上可见，创建并维护您或组织的信息图是一个有用的练习，该信息图将您的文档和与您的工作有关的信息归类。这将帮助您了解敏感信息的当前状态、以及谁可以访问它，这样才可能采取最有效的措施以保护它。

该 “信息图” 可以采用可定期更新的文本文档或电子表格的形式。

创建信息图时，请考虑以下问题：

1、这是什么信息？

这里的组织原则是将相似类型的信息组合在一起。例如，您可以确定所有财务凭证都属于同一类别，而并非所有电子邮件都属于同一类别。

根据信息类型对“内容”进行分组，很大程度上取决于您和您的组织的工作方式。也包括您在此处使用的软件，因为该软件本身可以被视为一堆信息，并且某些软件可以被视为敏感软件。

特别是对于“动态”信息来说，最好包括某些文档和通讯的元数据（例如图片和电子邮件附件），并考虑是否需要删除或修改它以保护您的隐私。

2、它在哪？

您的信息资产存放在哪些物理场所或实体中？这可能包括：办公室中的文件服务器、服务提供商处的Web服务器、电子邮件服务器、便携式计算机/电脑、移动硬盘、SD卡和手机。

3、谁有权使用它？

考虑当前的情况，而不是理想中的情况。例如，如果某人在办公室计算机上保存了报告文件夹，则有权访问该报告的人员可能包括：该人本人、负责维护服务器的任何IT管理人员、该人的知己等等。

4、它有多敏感？

有多种方法可以对文档的敏感性进行分类。为敏感信息建立明确的分类是必要的，别忘了带有关于如何保护它的明确说明。此处的目的是使您拥有一个始终如一地适合您的信息的量表，这将有助于识别最有可能受到威胁的数据、以及应采用的保护方法。

以下是一个3级规模的示例：

- 严格保密：只有特定的人才能访问此信息。对于此类信息有明确的责任链。

- 机密：此类信息不是供公众使用的，但是没有特定的必要以阻止组织的员工访问这些信息。

- 公开：此类信息不会对公众构成任何风险。但是，一般政策仍然涉及其完整性和安全性。

值得注意的是，在项目的生命周期中，所涉及数据的敏感性可能会发生变化。例如，如果您正在调查酷刑以便稍后对其进行公开报告，则其中涉及的许多细节最初都是严格保密或机密的。

在项目的后期，一旦收集了数据，必须保密的数据将与必须作为报告的一部分公开的数据分开。

根据这些问题考虑您的信息，您可以创建一个文档，该文档代表您当前的信息图。再一次，如前所述，请务必记住这是实时文档，应定期更新。

从下面进入本集的第一个练习，以逐步完成创建此类文档的步骤，并提供一个可能有用的示例模板。

最后

到现在为止，您已经做到：

- 列出了自己的盟友和对手，以及根据情况可能成为盟友或对手的中立群体

- 列出了您、您的盟友和对手之间已经建立的一些关系

- 建立了您自己的信息生态系统，该文档可帮助您了解信息敏感度的优先顺序，不论是静态信息还是动态信息。

下一集的内容将把这些分析转移到工作过程中遇到的威胁指标上，这些指标会提醒您潜在的威胁以及如何将您对这些威胁的知识系统化以采取行动。

[image]
[image]

每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局

[image] 关键词	威胁识别 时局
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月7日
[image] Description	教材

围观美国的选举对中国人来说有什么用？中国的反抗者需要从其他国家的抗议运动中了解到什么？

- Table of Contents

  利用指标，识别和分析威胁
  识别安全指标
  社会政治环境
  数字安全
  日常活动
  分享、分析和跟踪安全指标
  安全指标分析中应遵循的步骤
  识别和分析威胁
  分析风险，确定威胁优先级
  分析

欢迎回来！

在前面的内容和练习题中，您已经学会了如何通过分析您自己和您的对手 —— 从人到信息资产 —— 来确定最合理的保护措施所需要采取的逻辑。本集将开始与您一起更深入地分析威胁本身，之后才能真正进入行动。

[image]

利用指标，识别和分析威胁

帮助敏感人士监测安全状况的另一个重要工具是安全指标。安全指标是指您注意到的、可能对您的安全产生影响的任何异常情况。（在S03教程中看到这一概念的更多详细介绍）

安全指标可以包括具体的事件，如：收到直接宣告的威胁、对合作伙伴组织的攻击，或者您可能注意到的某些身边人的可疑行为；并且，它也包括更微妙的发展，如：您的设备状况的变化，或您的身体健康状况和心理健康状况的变化。

简单解释一下。关于您的电子设备状况的变化可能会预示着恶意软件感染、隐藏的监视状态被一些细节所暴露，您可以在这里看到简单的“基准线考察”方法：《如何识别手机上的恶意软件？》。

和电子设备一样，您的身体健康状况的改变也会预示着哪里出了问题，您应该定时体检、及时就医，一旦发现问题请仔细回想最近您接触过什么新的东西、是否服用了什么药物或改变了常规药物的使用，以尽可能寻找原因。

心理健康状况就更微妙了，我们每个人的心态都会随机地变化，但是，有些变化将预示着威胁或压力的出现。比如，您是否发觉自己的心态变得不那么积极了？曾经很有灵感，现在却似乎失去了斗志，觉得自己做什么都是无用的？身边的熟人变得冷漠？…… 您需要找找原因，是什么造成的这种情况。

是因为您发布的动员无人关注吗？有没想过为什么会这样，分析一下您的社交网络数据，您是否发现与您的影响力严重不成比例？这是否意味着您正在遭受影子禁令 —— 您的发布内容被限制阅读了？或者，您身边的人原本很亲近，却忽然冷漠起来了，在疏远您，您做了什么被他人误解的事吗？还是，有渗透者在背后制造内部矛盾、抹黑您的计划和立场、误导您的队友的认知？…… 找出那个人。

对于反渗透、心理安全、关系结构安全，本站有相关具体板块。

再比如，我发布一条推文："如果您讨厌警察，请转发本帖"。作为99%的我们这些老百姓，几乎每个人都讨厌警察 —— 那些1%的走狗；但您会转发这条内容吗？如果您不会转发，可能的原因是什么？

1. 比如，您也许不信任我，因为我不是您在现实中认识的熟人，您会担心我通过这样的动员收集您的意向，并顺藤摸瓜挖掘您的身份信息；您可能会因为表达了真实心意而惹上麻烦；

1. 想想看为什么您会产生这样的下意识回避？您曾经遇到过这种钓鱼吗？或者您身边的人遇到过？再或者，您通过IYP的内容了解到了 "社交媒体情报" 这种东西有多可怕？

1. 而现在我是一名活动家，我正在动员人们反击警察暴力、酷刑和强迫失踪的侵犯人权行为，如果上述担心在很多人心中存在，人们不会转发我的发布，这次动员就是失败的。

1. 您和我都需要对此进行思考：我需要思考为什么您会害怕转发？对于您的担心，我能做些什么？（从帮助您尽可能 匿名地使用社交媒体 、到 分身技巧 、到 动员策略 ）；您需要思考"担心"从何而来？可以采取什么措施以打破这种危险性？……这样， 您和我的思考就能走入同一个方向 。

如您所知此处可以举出非常多的例子，都是您和同道们很可能遇到的状况。您需要做的就是及时抓住这些信号，分析它们背后的真实原因 —— 而不是表面上的原因。不要被表面现象所蒙蔽。

所以，前提是您准确地知道 “正常” 是什么样的，也就是您的基准线，它需要清晰，它是判断标准。

简单说，上述这些变化的共同点是，它们可能表明您的安全状况发生了变化，应该在值得信赖的朋友和合作伙伴之间进行分享和分析，以确定其真实的意义。

不用担心，这并没有看起来这么复杂。我们每个人都习惯于监测周围情况，并注意到自己是否不再感到安全 —— 正如本教程第一集中所探讨的那样，我们对此有一种天然的直觉。而培养分析安全指标的做法，只是意味着要采取一种更加慎重的和有条理的方法。最好养成定期与同事和盟友记录、研究、分享和分析安全指标的习惯，因为这有助于您更客观地了解自己的安全状况。

识别安全指标

人们已经很善于注意到日常生活中可能出现的特殊问题 —— 这是您的直觉在起作用。但要知道，您的直觉并不总是万无一失的，这也是为什么要明确地建立一个“常态”的基准线的原因：分析并了解您在社会政治环境、数码设备、日常生活、身体健康、和情绪健康状态中所认为的 “正常”。

一旦那您建立了 “正常” 对您来说意味着什么的标准，就会更容易注意到环境中的变化 —— 即 您可能认为是 “不正常” 的东西。以下是一些建立基线和注意到这些不同领域的异常的提示。但是，请记住，是您而不是别人，才是最熟悉您自己所处环境的人，您应该相信自己的判断。

社会政治环境

密切关注您开展工作的政治、经济、社会、技术、法律和环境状况，对于确保您的安全和工作的持续成功至关重要。这是新闻和解密文件能带给您的最有价值的部分 —— 您需要做的就是，带着安全战略去

阅读它们，以您自己的利益为目的。

抓取局势中的机遇，助力您的事业；对局势中显示出的威胁及时作出反应，更新您的防御策略。后面我们还将更具体介绍这点。

监测您的社会政治环境的有益步骤包括与值得信赖的朋友、同事和同行组织交谈，跟踪和记录新闻，以及在开始新领域工作时与专家会面，等等。

数字安全

在数字方面思考基准线会比在现实中思考这件事更难一些。人们往往不会自然而然地识别出数字领域的安全指标，除非您是技术专业人士。于是您可能不得不相当慎重地对待它。

随着当权者对敏感人士越来越多地使用电子监控，学习如何寻找数字异常的重要性不言而喻。

在这里，和物理层面的步骤是一样的。首先建立一个基准线，了解您所认为的所有数字硬件（如电脑、电话、路由器、硬盘、服务器、智能家居等）的 “正常” 状态，以及您使用它们时的状态。监视以下活动的结果，定期检查和识别任何变化，看看它们是否相当于安全指标。

如果您怀疑有什么不对劲的地方，请向值得信赖的专家咨询。

- 使用反恶意软件程序扫描设备；
- 检查您的防火墙；
- 检查您的计算机是否有未经授权的进程或程序；

- 尽可能对在线服务使用两步验证；

- 如果设备必需离身，在设备上进行物理标记或使用防篡改带，并对其进行拍照，以帮助您验证是否被人动过（尽可能不要让设备离身）

具体安全知识可参见我们的 列表-5 “护盾” 栏目，那是专门服务于敏感人士的。本教程专注于您和您的组织曾经很可能没有采取的技巧和措施，不再重复具体步骤和常识。

日常活动

在日常生活中，有许多机会可以检查安全指标。每个人的习惯、例行公事和工作方式都不一样。

需要考虑的方面包括：从家到公司的交通方式、一天中做了哪些活动、随身携带哪些设备、以及与谁交流。通过对这些事情的思考，有可能从不同的角度来看待您的日常工作，并确定哪些因素可能意味着您的安全状况发生了变化。

下面进入本集的第一个练习，它可以帮助您建立基准线。

[image]

分享、分析和跟踪安全指标

与值得信赖的朋友、同事或合作组织分享和分析安全指标，对于帮助您识别是否存在任何模式，非常重要，这反过来又有助于您识别威胁。此外，这也是检查您的认知并努力保持其准确性的关键做法。

由于安全事件通常是 “敏感” 的，无论是作为资讯，还是对您的情绪影响，在“安全” 的空间中讨论和分析这些事件是很好的。考虑将安全指标列为会议的常规议程项目，以确保在必要时，可以对它们进行讨

论并采取行动。

使用下面的模式来指导对具体事件的分析，如被明确的威胁、攻击或事故。对于与健康和福祉有关的指标，建议以更非正式的方式进行分析，确保受影响的人在分享时能感受到被支持。

安全指标分析中应遵循的步骤

对于特别重要的安全指标（例如具体事件），提出以下问题作为分析的基础可能会很有用。

1. 发生了什么？

1. 什么时候发生的？

1. 在哪发生的？

1. 谁受到了影响？

1. 是否涉及基于性别、政治倾向、种族民族的暴力？对于涉及第三方的具体事件，这尤其重要。要考虑身体和心理两方面。

1. 如果发生侵犯性事件，谁应负责？

1. 为什么您这样觉得？尽量避免立刻进行指责，而是要确定事件的事实。

1. 它的起源是什么？这是否与常见的违规行为、环境因素、或您的人权工作和反抗行动有关？

您可以立刻使用您曾经或正在经历的事，做这个练习，比如 您的组织

中曾经发现过疑似渗透行为吗？记下您的发现，您从什么时候注意到某人的行为不对劲的？此人的行为影响到了什么和谁？它破坏了您和组织的反抗目标吗？还是破坏了您和队友之间的互信？您的判断真的准确吗？列出这些事实，检查其中是否有逻辑漏洞？…… 之后您就可以知道该如何采取行动。

（关于反渗透的详细内容，请参见本站专题板块）

无论您的工作情况如何，重要的是要建立一个空间，让您尽可能详细地记录安全指标，以便以后分享和分析这些指标。这可以采取文件或电子表格的形式，应定期分析（每周或每月），以便注意指标的任何趋势。您可以使用上述问题来帮助构建您的清单。该清单应被视为高度敏感！严格保密！

[image]

识别和分析威胁

对敏感人士的安全状况进行 “诊断” 的最后和最详细的工具是：威胁分析。如前所述，这里的威胁指的是会对您自己或您的组织的工作造成伤害的任何潜在事件或事故。

将前面的所有练习付诸实践，应该可以帮助您很好地了解自己所面临的威胁。

接下来我们将对这些威胁进行明确的命名，根据它们的可能性和潜在影响来确定它们的优先级，并详细分析它们的潜在原因和后果。

所有这些都将帮助您确定正确的策略，以防止它们发生，或在它们发生时及时做出反应。因此，您的安全计划应该是预防和应对策略的结合，使用这些策略来降低威胁成为现实的可能性，并在威胁发生时减少其造成的影响。

与前面的所有步骤一样，这往往是您在日常生活中进行的事，但不一定要明确地表达出来。这个过程只是为了更加慎重和详细，以促进对您的做法进行批判性思考。

请记住，这可能是一个情绪化的过程，但采取措施识别和应对您所面临的威胁可以而且应该是一个增强能力的步骤。威胁也可以是您工作有效的标志；有效到让您的对手害怕了，想要阻碍它。

您可以从 “已知” 的现有威胁开始，并仔细检查它们。从下面按钮进入本集的第3个练习，针对现有的和潜在的威胁，展开您的头脑风暴。

分析风险，确定威胁优先级

如上所述，可以根据以下各项查看威胁并将其分类：

- 威胁发生的可能性
- 是否有影响、什么时候产生的影响

可能性和影响是可以帮助您确定风险的概念：威胁的可能性或影响越大，风险就越高。如果威胁的可能性较小或影响较小，则风险较低。

以这种方式对威胁进行分类可以帮助您避免感到不知所措，并使您对威胁的看法保持现实。同样，与他人分享您的发现以检验您的看法也是非常好的。可能有助于可视化您在 “威胁矩阵” 中列出的内容，如下所示：

[image]

接下来您就可以对上述步骤列出的威胁进行更深入的分析，确定发生这些威胁所需要的条件及其潜在后果，这将有助于您计划对这些威胁做出哪些最有效的反应。

分析

您可以将从对环境的最广泛分析开始这一过程：观察与您的工作相关并可能影响您的安全状况的社会政治，经济，社会，技术，法律和环境发展。

为此，可以每天早晨简单地阅读新闻，或者与可信赖的朋友或同事谈论他们的观察结果。而且，还可能包含更复杂或敏感的任务，例如执行您自己的调查研究。比如您在社交媒体上被水军瞄准了，您想知道背后的人是谁吗？他们的目的最有可能是什么？他们的关注点针对您的哪项活动或观点立场？…… 了解这些，做到知己知彼。

通过这一过程，您获得的信息自然会为您和反抗组织做出的决定以及您作为激进社区采取的战略、计划和行动提供重要见解。

请注意，在进行和持续的情况监视时，重要的是要考虑您的信息来源：媒体是客观信息的可靠来源吗，还是您必须使信息来源多样化？同事、朋友和合作伙伴组织，以及学者、专家、友好的其他国家当局和使馆，与安全相关的电子邮件列表、旅行社 ……等等，也都可以作为您的策略和安全相关的丰富背景信息来源。

定期对局势进行更深入和有意识的监测和分析，也是反思您的安全局势的一种好方法。它帮助您将工作和战略置于其正在进行的地方 ——区域、国家和全球发展中，并确定那些可能表明安全局势发生变化的因素。（比如一期工程中的“纸条”部分）

全球发展也要计算在内？是的。没有人是在真空中存在的，每个人都与周边的一切产生关系，甚至在本教程的主题上，这一 “关系” 甚至没有因距离的拉大而减弱。

您还应该从中分析寡头公司的社交媒体服务如何审查内容、算法如何通过推高一些内容而降低另一些来引导舆论和转移人们的注意力，更有，选举后的维稳镇压计划如何进行，异议活动家应该做好什么准备…… 这些分析都是基于您的利益的思考，将为未来在您的本土实践民主时提供重要的基础能力。

再比如，中国人为什么要关注美国的抗议运动？因为，如您所知，全世界只有两个国家能实现最新进的全套维稳战术：中美。BLM 运动不仅提供了对此种维稳能力和其思考方式的密集呈现，并且，行动者也演示了丰富的应对技巧。这些应对技巧都可以作为未来中国的反抗者的参考书。

尤其是，鉴于中国当局非常擅长模仿，您知道，他们从来都倾向于模仿最具危险性的手段。

所以，您应该知道该如何使用我们制作的 **“通过BLM”** 系列的内容，不要把它当成普通新闻去读！IYP的列表-5 中有 “维稳面面观” 板块，其中收集的内容都应该作为中国活动家的 “威胁响应” 计划的一部分 —— 放在您的最敏感行动计划部分里。

[image]

态势监测和分析是安全计划的 “引擎”，从中您可以确定将对自己的战略产生影响的关键发展。

您需要关注的主要进展包括：

- 新的参与者的出现（比如新上任的政客等）
- 新披露的电子监控方法或技术，找到避免它的方式
- 新出现的维稳手段和操纵手段
- 关键角色的话语，关于他们如何看待您的工作的新态度

有许多可用于情况分析的框架。通常在战略计划的背景下进行的是两种常见的情况分析：**PESTLE**（政治，经济，社会，技术，法律和环境）；或 **SWOT**（优势，劣势，机会和威胁）分析。

本集的第4个练习们将进行简要的 PESTLE 分析，并尝试找出您应该意识到的去年以来的关键发展。

[image]
[image]

草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性

[image] 关键词	威胁响应 威胁模型
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年3月14日
[image] **Description**	教材

世上并没有百分百的安全，威胁行为者更多拼的是财力和实力，于是您需要
最大程度上增加他们攻击您的成本，耗尽他们的财力和精力，您就赢了。

- Table of Contents

  威胁、能力和脆弱性
  现有做法和能力
  找出差距和漏洞
  安全策略：为您的敏感工作留出空间
  能力建设和外部资源
  外部培训和顾问
  选择培训或培训师
  安全的物质资源

[image]

欢迎回来！

前文中我们和您一起分析了所有可能发生的威胁和发生形式 —— 从

来自人身的到来自技术的，接下来就可以开始分析如何应对这些威胁了。

在建立安全策略时，人们从来都不是从零开始的；您的直觉一直都在日常生活中帮助您避免威胁或应对威胁，此外，您还有某些社会化的实践 —— 即 “常识” —— 有时候也可以使您免受伤害。比如，群体事件发生时要做好应对断网的准备。

再比如，一些中国互联网用户有这样的 “常识”：如果您在社交媒体上的言论忽然遭遇大批水军围攻，那么就需要警惕稍后可能会有警察上门。

但这显然是不够准确的判断，它来自于人们所了解的发生在他人身上的一些前车之鉴。如果您就此认为 “如果我没有被水军围攻，就没必要担心警察上门”，那就是错误的：我们称之为 “虚假的安全感”；反之，如果您经常遭遇水军围攻，因此经常陷在担心警察上门的恐慌中，那也是错误的：这是一种凭空制造的压力，长此以往您的身心会受到明显伤害，恐慌导致愈发难以判断真正的威胁 ，难以及时准确地作出反应 —— 而这正是维稳警察最期待的 “效果”。

在本集中，我们将考虑这些做法以及您的其他能力，尤其是您的弱点，以培养批判性思维，避免错误的 “安全感”。

为了从本集中获得最大的收获，请确保您已经完成了上一集中的背景分析练习。

威胁、能力和脆弱性

为了制定应对您所面临的威胁的措施，可以从使您更容易或更不容易受到这些威胁的因素来考虑。这些因素就是您的能力和脆弱性：

- 能力有助于使您更安全地抵御特定的威胁（即 降低其可能性或影响）

- 脆弱性会使您更容易受到威胁（即 增加了威胁的可能性或影响）

能力和脆弱性可能来自您自身、也可能来自其他行为者、或者您所处环境中与您的安全有关的特征。比如，如果您的爱人有点不够沉稳，心里藏不住话，那么TA就可能是您的 “脆弱性”；再比如，您的办公室网络升级了一系列安防措施、并对成员进行了安全培训，就会为您和其他同事带来 “能力” ……

一旦您确定了这些特征，就可以采取行动，以减少脆弱性、并建设您的能力，以最大限度地降低威胁的可能性或影响，从而最大限度地降低每一种威胁所带来的风险。

现有做法和能力

如上所述，步骤是首先评估您目前的防御做法和能力。大多数人在日常生活中已经采取了一些基本的安全措施：比如锁上办公室的门和为自己的在线账户设置强大的密码，等等，都是安全措施。但是，必需努力避免自满 —— 虚假的安全感是危险的。非常建议采取批判性思考，想想看自己现有的做法是否与您在前文的练习中所发现的威胁直接相关？是否已经将压力水平和保持您的整体健康的标准考虑在内了？

考虑一下哪些＜能力＞与您已经确定的威胁的不同方面相对应 —— 比如：

- 在司法骚扰案件中：您具有良好的法律知识

- 在被没收电脑的情况下：您有加密的硬盘、隐藏的加密分区设置妥当

在下面的练习中，您可以开始回顾您已经确定的威胁以及它们的表现形式 —— 谁和什么会受到影响？会在哪里发生、如何发生？威胁来

自谁、它将产生什么样的连锁反应？ —— 根据您已经拥有的做法和能力进行评估。

[image]

找出差距和漏洞

下一步要从一个稍微困难的问题开始。还有哪些差距可能使您容易受到这些威胁？您的哪些无益的心态或缺乏足够的知识或技能是您的 ＜弱点＞？

考虑和确定自己的弱点在情感上可能是一个艰难的过程。然而，这种洞察力将有助于您更准确地确定自己需要建立的新资源和技能，以改善安全性。

在思考这个问题时，请记住，如果缺乏足够的信息，或承受压力、恐惧和创伤，可能会导致您产生毫无根据的恐惧或未认识到的威胁。

您必须努力在掌握信息和过度思考之间取得平衡。可以采取一些步骤，通过小组讨论、或与值得信赖的盟友和朋友交谈，来检查自己的看法。

根据您在前面练习中的分析，可以反思自己所知道的有关自己所面临的威胁的细节，以及预防或减轻这些威胁的现有做法。

从下面进入本集的第2个练习，它旨在帮助您找出自己与每种威胁有关的 ＜差距和弱点＞。

安全策略：为您的敏感工作留出空间

有效的安全战略和计划必须符合您开展反抗工作的具体政治、经济、社会、技术、法律和环境背景。

如前文所述，政治威胁来自其他行为者，这些对手的利益可能会受到您的工作的影响，因此他们打算封锁您开展工作的社会和政治空间。安全策略可以帮助您确定对手接触的策略，以维持或扩大这个空间。

思考三大类型的安全战略是有用的：

1、接受战略涉及与其他行为者 —— 盟友、中立方和反对者 —— 接触，以促进社会对您的反抗活动的容忍、接受度和最终的支持。这通常是通过倡导活动、运动、交涉和教育活动进行的。

2、保护战略强调学习或实施新的方法和做法，重点是捍卫您的工作空间。这也可能意味着利用您的盟友的力量来进行保护 —— 合作很重要，并弥补您现有安全做法中的不足。

3、威慑战略的重点是提高对手攻击您或您的工作的成本 —— 无论是金钱成本、名誉成本还是其他成本。这些战略在很大程度上还取决于宣传、运动、交涉和教育活动，并要求您有一个完善的威胁行为体图谱，以便知道哪些盟友可以帮助提高攻击您的成本。这就是您在前面练习中已经完成的部分。

许多安全战略和计划将包括属于上述两类或所有三类的活动：当然，这取决于您所确定的背景和威胁。

从下面进入本集的第3个练习，将您想要建立的防御能力（在前面练习中确定的东西）与最适合您工作的战略目标相匹配。

[image]

能力建设和外部资源

一旦您确定了按照上述总体战略解决安全方面的差距和脆弱性的方法，就可能需要进行某种形式的能力建设了。这可能意味着学习一种新的技能，也可能需要长期改变您的工作方式。

考虑以下有助于促进行为改变的因素：

1、福祉：不仅意味着敏感人士的身心处于可以积极学习的条件下，而且还包括，拥有足够的时间和安全的学习空间。

2、态度：您在多大程度上认为这一学习过程是有价值的、有用的和合乎逻辑的？请记住，态度是主观的，可能会受到压力、恐惧和创伤经历的不利影响。

3、知识：对您所处的政治、经济、社会、技术、法律和环境背景的深刻理解，使您能拥有建立新能力的坚实基础。

4、技能：您能够参与和操控环境的核心。这些技能可能包括身体健康和自我照护、政治动员的技能、使用加密技术的技能，以及更多。

5、资源：在很大程度上影响着您改善上述要素的程度。想一想您和您的同事可以利用的任何资源，以及在必要时如何获得其他资源以进行能力建设。

外部培训和顾问

培训和外部顾问在帮助组织和网络制定安全计划和技能方面往往非常有用。我们提供的培训材料都是免费的，但如果您需要现场培训和实操，那可能会比较贵；如果您的组织内部沒有人能提供相同技能或培訓，依旧值得作出这样的預算。

最好的顾问会针对您自己的安全情况赋予您权力，而不是为您提供所谓的“简便的解决方案”！利用他们来培训您认为与您的活动相关的工具和策略，并弥补您现有安全策略的不足。

请注意，外部顾问不应该在没有组织成员参与的情况下，对您的机构的安全实务进行分析，也不应替您作出改变或决策。

选择培训或培训师

亲密朋友、和您一起从事敏感政治工作的同事、值得信赖的国际组织，都是选择安全问题培训的良好建议来源。

试着对您期望学到的东西有一个明确的想法，但要尊重培训师的意见，即在给定的时间框架内可以实现什么。

在您决定聘请他们之前，请考虑他们应该具备什么样的经验或知识。考虑语言、时间、地点和后续行动的选择等因素；之后您是否有时间练习或使用新技能、知识或资源？练习非常重要，只有您行动起来才能真正掌握这些技能。

在您的组织内讨论这些问题，以达成一个对大家都有效的解决方案。如果一些成员不感兴趣，就会对培训产生负面影响，并会降低随后可能产生的效益。

我们不会阻拦您进行在线远程培训的尝试，如果您认为现场培训非常危险的话 —— 有些情况下的确如此。但您真的需要斟酌在线培训的效率问题 —— 它可能会奇低。在线会议软件的安全性是另外问题。

安全的物质资源

建立和提高您的安全能力往往会产生财务影响，并可能给已经捉襟见肘的资金预算带来压力。无论是更换硬件受损的新笔记本电脑的费用，还是培训费用，最终您的安全都可能需要钱。

有一些组织会向需要解决安全问题的人权维护者提供财政支持，申请过程有点复杂，而且需要时间，您需要考虑到这些；并且尽可能令您的申请过程保持私密，因为比如在中国，申请外国组织的资金很有可能被所谓的 “间谍法” 捕获，在当局想要惩罚您的时候拿出来作为把柄。

对于相关资源，在这里下载一份手册：《New Protection Manual for Human Rights Defenders》。

下一集中我们将继续讲解创建安全计划和协议的一些方法，并推荐练习以帮助您找到最适合自己和团队的方法。

[image]
[image]

充分的准备和应急反应同样重要：整体安全S01E07 - 计划是“活的”

[image] 关键词	团队 威胁响应 防御
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年4月2日
[image] **Description**	教材

虽然安全计划和协议是重要而有用的工具，但如果情况需要，灵活地放弃它们的能力同样重要，甚至更重要。

- Table of Contents

  安全计划和协议的要素
  预防威胁
  紧急应变
  福祉和设备
  团体和组织的安全
  创建和维护安全计划
  团体和组织的应急计划
  1、紧急情况的定义
  2、角色和责任
  3、沟通渠道
  4、预警和响应系统
  改善组织安全管理

欢迎回来！

本集开始将和您一起制定安全计划和协议。

[image]

一旦您明确了您和组织在活动中所面临的威胁，就可以开始将您的需求组织成安全计划或协议。这些计划可以是正式的书面文件，也可以是非正式的共享协议，但无论哪种方式，它们都应被视为“活的”，并应定期更新和审查。

您可以根据任何适合您的逻辑来组织这些计划和协议，例如按您的反抗活动、按您组织动员的地区、按人、按星期、或按照任何其他符合您工作方式的标准。无论您如何安排自己的计划，所有好的计划都应该包括一些共同的要素。

安全计划和协议的要素

大多数好的安全计划都能达到以下一个或两个目的：

- 预防威胁 —— 这些策略旨在防止已查明的威胁发生 (即减少其可能性)。

比如，您穿上了防弹衣，就是为了防止/减少可能的大规模枪击威胁的影响；您制作了并熟练使用了加密卷，就能防止/减少电脑被警察查抄后重要资料丢失和您被起诉定罪的威胁。

- 应急反应 —— 也称为应急计划，是您在威胁成为现实时所采取的行动。这些行动的目的一般是减轻事件的影响、减少事件发生后的进一步伤害，并阻止侵略者 (如果有的话) 进行进一步的伤害。

比如，您在参加抗议活动中被便衣警察瞄准了，他们想要抢走您的设备，于是您快速禁用了生物识别功能；这就可以让警察费点劲、甚至很难打开您的手机；再比如，您在办公室里不仅配置了明显的监视摄像头（比如在屋顶的墙角上）而且配置了隐藏的摄像头，这样一来，

即便闯入者迅速毁掉了那些明显的摄像头，您的隐藏摄像头会继续工作，以记录下闯入者的行为。

对于您在前面的练习中已经识别出的每一种威胁，您通常应该同时具备预防和应对策略。

下面我们将更详细地探讨这在不同情况下可能意味着什么。

预防威胁

许多预防策略将反映您的接受、威慑和保护（或自卫）战略。这些策略可能包括宣传您的抗议运动、或其他形式的与公众或民事/军事当局的接触，以提高人们对您的工作的认识和接受。或者，这些措施可能涉及加强您与盟友的联系，或采取其他策略，建立您自己的能力和灵活性。

这些措施一旦实施，很快就会成为您的工作和个人生活的一个“正常”方面，尽管可能需要时间来适应。

紧急应变

要知道，即使是最好的计划也可能会失败。有些时候，也许是由于环境瞬息万变，尽管您已经尽了最大的努力去预防，但还是会遇到侵害或事故。于是您需要 PlanB。有了应急预案，您就可以有条不紊地应对安全事件，并限制伤害。

应急预案通常都是针对具体案例的。正如前文中所讨论的那样。诸如轻微犯罪或自然灾害等因素可能会严重影响您的工作，也是许多敏感人士经常遇到的威胁，因此，如果您认为这些威胁已经构成风险，就必须制定应急计划，以应对这些可能发生的情况。

一些简单的例子可能是，比如手头有一个可信赖的好律师的联系方

式，商量好在抗议活动期间被捕时发送加密的警报信息，或者只是在办公室里准备一个急救箱，以防携带武器的闯入者导致您和队友受伤。等等。

福祉和设备

至关重要的是，要包括您自己的福祉、和管理您的设备和信息的策略。

应该考虑采取哪些行动来保持您的体力，并对您的工作和安全保持一种完整的关注，例如，安排吃饭、睡觉、放松和享受的时间和地点，不要忘记这些因素同样重要！您还应该考虑开展工作所依赖的设备 —— 不论是电脑还是打印机、扫描仪还是录像机，以及确保能够控制谁可以访问您的信息和通信的策略。

[image]

下面是一个敏感人士简单安全计划的例子，帮您了解所有这些在实践中看起来是什么样的。

目标任务：收集侵犯人权行为受害者的证词。

地点：在农村地区。

威胁 —— 被警察骚扰或逮捕。

- 被没收电脑、手机。
- 因此而丢失数据。
- 损害受害者的匿名性。

预防策略 —— 行动和资源

- 提醒同事、友好的大使馆和国际组织，关于行动的时间期限和地点。

- 将地方当局/侵犯人权责任人的详细联系资料提供给大使馆和国际组织。

- 每12小时与同事签到一次。

- 证人证言将被立即保存到加密卷中。

- 证人证言会用GPG加密后发给同事 —— 每天晚上固定时间发送。

- 邮件收件箱和已发文件夹在使用后将被彻底清理。

- 安全指标和签到将通过安全的端对端加密通讯共享。

应对策略 —— 行动和资源

- 编写警报信息 (暗语)，以便在发生被监视/被跟踪的情况下发送给接应您的队友。暗语是只有你们两人能理解的话。

- 准备好被捕时发送的警报信息（代码/暗语）。

- 将律师的号码放在快速拨号上。

应急预案 ——

- 如果被抓，要发警报信息给同伴，并打电话给律师。

- 同伴在收到报警信息后，会向盟友组织报警 —— 使馆和国际组织等。

- 要求国际组织发出紧急呼吁。

- 如果在发生致命威胁的情况下，要交出的加密卷外层密码。

福祉方面的考虑 —— 您的心理健康是能否敏锐反应的决定性因素

- 在当地一家体面的餐馆吃饭，每天至少两次（selfcare + 保存您的体力）

- 在用餐时间关闭手机和所有其他设备（享受当下）

- 每天晚上通过安全渠道给家人打电话联系（家庭是坚实的后盾）

设备和信息 ——

- 手机上有加密的通信应用

- 具有加密卷和加密电子邮件的电脑，并具有如 GPG 这样的功能

请注意，上面的例子仍然意味着盟友的密切合作、协调一致的行动，以建立一个新的联盟。不要让自己孤立无援。

当涉及到团体或组织时，规划的过程可能会涉及一些额外的步骤，以确保团体动态不会受到负面影响。

如前面的内容所述，拥有坚实的最新安全计划是您的复原力和灵活性的重要补充，但是，不能取代它们。除了详细的分析和规划外，您还

必须为意外情况做好准备。虽然安全计划和协议是重要而有用的工具，但如果情况需要，灵活地放弃它们的能力同样重要，甚至更重要。当出现您没有 —— 或不可能 —— 计划到的情况时，培养中心意识和冷静是关键。

[image]

团体和组织的安全

团体和组织具有复杂的内部动态和文化，影响着您的互动方式和安全计划。当您考虑到，作为一个群体，在工作过程中，不愉快的事发生在自己身上的真正可能性时，这可能会变得更加复杂。

在一个群体中进行安全规划可能会带来压力和情绪化，担心显得过于偏执是很常见的。从实际情况来看，在小组中进行分析并达成协议也是很困难的。为了使安全计划成功，需要每个人都能认同，但在团体中，这可能是一个高难度的任务！

在此，我们将探讨在团体和组织内建立和改进安全策略和计划的一些关键问题。

创建和维护安全计划

一旦小组进行了风险分析（使用前文练习中概述的工具），在制定安全计划时，您可以记住一些要素：

- 实现协调 —— 合理地介绍您的计划，并与您的同事讨论每一个步骤。安全是一个非常情绪化的问题，我们每个人对它都有不同的看法，这意味着谈论它是一个需要时间和安全空间的话题。尽量不要吓唬人，但要给人们提供事实，并创造一个平静的空间，让人们提出问题和关切。

- 参与式设计 —— 有些人可能不欢迎未经他们协商就决定的安全

计划。高风险的活动和紧急情况可能会让人感到痛苦，重要的是每个人都要对自己被分配的角色感到满意，如果不满意，也能有一个空间可以提前表达自己的担忧。在计划还在制定的时候，尽量让更多的人参与进来。

- 角色扮演 —— 在某些情况下，设计一个角色扮演，使组织成员能够练习如何应对某种情况或紧急情况，可能是有用的。然而，要谨慎行事，确保每个人都愿意参与，因为角色扮演可能会引发过去经历过创伤的人的情绪反应。

- 重新规划和考虑 —— 请记住，所有安全计划都应被视为“活的”，并应定期进行重新评估和讨论，特别是在新成员加入小组时。包括固定的日期来审查您的安全实践和计划，并确保安全不是事后的想法，而是您的战略计划的核心。

团体和组织的应急计划

制定紧急或应急计划是至关重要的，因为没有任何预防措施能在任何时候都100%有效。在制定这种计划时，要考虑到以下关键因素：

1、紧急情况的定义

决定什么是“紧急情况”—— 即我们应该开始实施计划中的行动和应急措施的时间点。这一点很重要，因为有时会不清楚 —— 比如您想象一下这样的情况：在外地任务中与同伴失去联系，您会等多久才宣布紧急情况？

2、角色和责任

给每个人分配一个明确的角色，并让他们事先知道并同意 —— 这将减少事件发生时的混乱和恐慌。在每一种威胁的情况下，考虑您可能必须承担的不同角色，以及应对紧急情况时的实际情况。

在此范围内，应对紧急情况的一个重要策略是启动一个支持网络 —— 一个由您的盟友组成的广泛网络，其中可能包括朋友和家人、社区、当地盟友、以及国内或国际的盟友，如非政府组织和国际独立记者。您的盟友如何支持您？您是否应该事先与他们联系，确认他们是否愿意在紧急情况下帮助您，并让他们知道您对他们的期望？

3、沟通渠道

协调对紧急情况的反应总是涉及协调行动，因此数字通信越来越重要。决定在不同情况下与每个行为者进行沟通的最安全、最有效的手段是什么，并确定一个备用手段。

在紧急情况下，制定明确的指导原则可能会有帮助：

- 沟通的内容（要点）
- 使用哪些渠道（尽可能安全；如果无法做到，要使用暗语/隐写）
- 对谁（在前文中您构建的盟友清单中位居前列的选项）

4、预警和响应系统

这是一个有用的工具，可以协调您对紧急情况或迫在眉睫的高风险情况的反应。

早期警报及应变系统基本上是一份高度保密的文件 (不论是电子形式还是其他形式)，在发生紧急情况时可打开，用以记录所有有关安全指标和已发生事件的详细资料，清楚说明计划中的应变行动和次序，以及所要达到的指标。它还应包括为保护有关人员免受进一步伤害和帮助他们身心康复而采取的善后行动。

早期预警和反应系统提供了有用的文件，以便随后分析所发生的事，以及如何改进您的预防策略和今后对威胁的反应。

改善组织安全管理

各组织必须将安全管理以及管理人员、工作人员和志愿者对安全管理的执行视为一个持续的重新评估过程。

建议您定期评估您的安全策略和计划在多大程度上不仅与您的运作环境相一致，而且还被您的成员所接受和实施，这会很有用。在下一集内容中我们将更多介绍关于评估一个组织的安全性的信息。

[image]
[image]

安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动

[image] 关键词	团队 行动
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年4月3日
[image] **Description**	教材

只有当您的队友能主动积极地采取您所支持的科学的安全措施时，真正的安全才能实现。不能要求人们把它当成任务来做。

- Table of Contents

您的组织安全吗
评估标准
克服对安全计划的抵制
安全性与DNH方法
行动与资源
行为和隐含的道德信息
1、不同的人有不同的价值观
2、恐惧、紧张和不信任
3、资源的使用
4、文化特征
抗议活动：准备，分析和计划
做好准备
了解所有行为者
分析风险
明确计划

本集的教程将从上一集的个人角度转向组织角度。

[image]

您的组织安全吗

作为一个组织，您很可能已经采取了一些安全措施。同时，您可能在考虑是否有改进的空间 —— 通常都是有的。该从哪里开始这个问题可能会让人不知所措，所以，最好先进行一次评估，对您现有的组织安全进行现实的概述。

在评估过程中建议您加入一些外部顾问来协助指导这个过程，也许会有帮助。举例来说，您应该考虑：

- 内部—— 管理层和高级工作人员、正式工作人员和志愿者；
- 外部—— 捐助方、外部顾问和培训师。

让这些行为者参与其中，各有利弊，重要的是，这个过程要以包容、协作、透明和非评判的方式进行。

组织内的正式或非正式等级制度需要对自己的计划和 “现场” 工作人员或志愿者的需求保持敏感，前线人员在日常工作中可能面临更大的风险。工作人员和志愿者也应尊重这样一个事实，即 管理层在使安全方法标准化方面面临的是一项艰巨的任务。互相体谅很重要。

评估标准

您可以从研究一些具体问题和指标开始，以帮助评估组织成员如何遵守安全协议。请考虑以下几点：

1、获得的安全经验。您的组织成员是否有实施安全做法的经验？是

所有人基本都有这类经验吗，还是只有少数人具备这样的经验？

请注意，这里所指的是实践安全措施方面的经验，而不是遭遇威胁方面的经验，现实中很多敏感人士容易混淆这两者。

比如一个敏感人士的组织中所有人都曾经遭遇过警察的胁迫和威胁，最终他们的确躲过了危险，但这并不意味着他们具备实施安全做法的经验。尤其是，您的对手的手段在不断升级，如果没有不断主动更新自己的专业的安全措施实践，曾经遭遇威胁的经验并不能帮助您解决未来可能面临的问题。

2、态度和意识。您的队友们是否意识到了安全和保护的重要性？他们对安全和保护的态度是否积极？是否愿意做出改进？他们认为存在哪些障碍？对于数字安全、实体安全和心理-社会福祉的态度和意识是否在整个组织内共享？

意识很重要。您无法通过观察来了解您的队友的想法，你们需要就此进行坦诚的交流，尤其是，让队友提出问题和需求，作出深入的探讨。采取倾听的方式，而不是您来告知大家该怎么做，即便您的想法是正确的。

如果您的队友态度很消极，您需要知道为什么，应该在哪里给予帮助。

3、技能、知识和培训。需要为培训提供资源、时间和空间（正式或非正式的）。组织成员是否可以获得此类培训？培训是否同时包括社会心理健康和数字安全方面的知识和技巧？

如前面的章节所讲述的，社会心理健康不仅是重要的，而且是维护安全必不可少的基础。任何人在焦躁和绝望的情况下都无法作出最佳选择，如果无法掌握心理状态，您的灵感就会被抑制，尤其可能作出糟糕的和让自己后悔的决定。

敏感人士长期在威胁的高压下工作，精神心理出现问题毫不奇怪。习惯了压力状态的人自己也很难识别到压力，这就是为什么我们前文中

的练习首先希望教会您如何客观地评判自己的精神心理状况。这对安全来说很重要。

培训的目标不仅是要帮助人们掌握技能，并且尤其重要的是，要帮助人们培养一种科学的敏锐度，能主动觉察到什么情况下应该采取什么样的措施。

4、安全规划。安全规划在多大程度上被纳入您的组织工作？多久进行一次环境分析和制定安全计划？计划是否定期更新？是否包括数字设备管理和队友压力管理？

5、职责分配。是否对执行您的安全做法有明确的责任分工？这些责任在多大程度上得到了遵守、有哪些潜在的障碍？

通过协作才能获得最好的组织安全性；确定每位成员的任务范围，您将很容易查找到出现问题的地方和相关责任人。

您需要确保人们愿意遵守规则，这意味着您为每一位成员分配的任务是其本人力所能及的，且具有足够的信心，如果不是这样，您需要及时交流以了解原因，并作出合适的调整。

6、所有权和合规性。人们是如何参与组织安全规划的，他们在多大程度上遵守了现有的计划？这里出现的问题是什么，如何克服这些问题？如何使这个过程更具参与性？

不要担心出现问题，管理团队并不是那么容易的，如果人们对您的提议表现淡漠，您需要知道为什么。只有当您的队友能主动积极地采取您所支持的科学的安全措施时，真正的安全才能实现。不能要求人们把它当成任务来做。

7、对安全指标和威胁事件的反应。您的团队中多久分享一次安全指标？如有必要，多久对它们进行分析并随后采取行动？

这要因人而异，您肯定知道对于您的组织来说，什么样的频率是最恰

当的。

8、定期评估。您的组织多久更新一次安全战略和计划？是否有具体的程序，还是临时性的？如何使其更加经常化？还存在哪些其他问题，尤其是，如何克服这些问题？

尝试与您的队友一起完成以下练习，以探索遵守安全计划的程度，并找出在执行不佳的情况下人们发现的障碍。

[image]

克服对安全计划的抵制

在引入新的安全协议时，您可能会遇到来自组织者、工作人员或志愿者的阻力。他们可能会对变化不满意，而您应该倾听他们的理由。

请记住，安全是一个非常个人化的概念，人们可能有抵制某些协议的个人原因。新的措施可能需要学习新的技能，也许人们觉得这具有挑战性；另一方面，如果您的团队对权力动态和等级制度的处理不当，也可能会产生影响。

您需要仔细分析以了解常见的形成阻力的观念、其根本原因、和可能的应对措施，以帮助克服您的团体、组织或社区中的阻力。

安全性与DNH方法

接下来我们将考虑您的安全措施—— 新旧措施 —— 如何对冲突产生积极或消极的影响，不论是对群体内部还是外部的影响。

这里使用的 “冲突” 一词可以指代武装的、也可能是非武装的冲突，人们所遭受的暴力可能是身体上的，也同样可能是经济上的、或基于性别的、或制度上的、结构上的、心理上的或其他方面的。

有时，活动家群体也会受到组织或运动内部冲突的影响（比如性骚扰）。在某种冲突（也许是多种冲突）的背景下工作，您的行动和行为可能加强人与人之间的联系、也可能会制造人们之间的分裂，这反过来又会影响冲突本身，使其缓解、或者恶化。

作为活动家，您应该寻求增加您的行动的积极影响，减少可能的消极影响。不伤害（DNH）方法可以帮助您实现这一目标。

该方法假设您的所有行动和行为都会导致积极和消极的后果。

行动 ＋ 行为 ＝ 后果

在本集中，我们将考虑您的行动和行为可能对这些冲突产生积极或消极影响的一些方式，特别是在组织层面上，由于您对安全做法进行了改变而产生的影响。

行动与资源

您的行动可以理解为您在现有局势下所做的一切，包括您获得、使用和转让的资源。事关安全和福祉的资源往往被认为是宝贵的，而获得这些资源的机会可能是有限的。当您寻求在您的团体或组织内扩大行动和资源时，请考虑这些变化可能产生的影响 —— 影响可能并不总是积极的。

下面我们将探讨一些负面影响会如何出现，以及如何应对这些影响。

1、竞争与包容 —— 只向选定的个人提供资源可能会增加现有的紧张关系，或造成新的紧张关系。如果您在使用和分享资源方面能够具有更多的包容性，就能将人们联系起来。如果无法共享资源，就和小组讨论为什么，并得到人们的认同。

恶化的竞争是您在社交媒体上看到的非常熟悉的东西。社交媒体不是

社区，而您的组织必须是社区，人们应该在这里自然感觉到被关爱和存在，没有人应该被边缘。在资源分配方面将非常容易体现这点，您应该倾听和尊重所有人的意见。

2、替代与欣赏 —— 引入新的实践或实施新的资源可能意味着旧的实践、传统、甚至人们熟悉的角色，被取代。现有的战略和资源只有在合理的情况下才能被取代，并且要尊重您的队友为之付出的努力。

比如，如果您找到自动化的培训方式，而终止了人力培训的旧流程，培训师、助理和相关队友的角色都会被取代；也许您可以说出很多理由关于为什么这种改变是值得的和必要的，但如果现有的人力培训流程效果很好，您就应该重新考虑您的建议。尤其是，您必须承认并真诚地感谢一直以来在此工作的所有人。这些伙伴应该被提升，而不是被废弃。

3、选择性和权力关系 —— 让整个团体或组织参与讨论关于谁可以获得培训机会或其他利益，可以提高对安全措施的接受程度，并加强整个团队的团结意识。

不必怀疑，您所在的社会的等级制度和传统思考方式或多或少都会影响您的组织和社区，您需要努力避免那些糟糕的影响。尽可能保持权力关系公认合理，尽可能流程透明。

4、生活和工作标准 —— 如果用于安全和保护的资源被用于那些已经享有较好生活或工作标准的成员，可能会导致团体内的进一步分裂。

请认真考虑：谁应该接受哪些培训？谁可以为哪些活动获得报酬？谁从安全中获益更多？由于生活在城市（而不是农村）环境中，谁能更好地利用通信和其他基础设施？如何消除这些差异？在跨区域联盟中这些问题尤其重要。

[image]

行为和隐含的道德信息

在本教程的第6集中，您已经练习了如何培养能力，并弥补缺陷。在建设自己的能力时，您应该考虑您的行为可能会如何改变，以及这可能会如何影响他人。

您的行为会向您所在领域的所有行为者 —— 包括您的盟友和对手 —— 发出非语言的、隐含的信息。对这些信息的解读，就像您的行为本身一样，会导致群体内的进一步联系或分裂 。

下面我们将探讨发生这种情况的四种常见方式。

1、不同的人有不同的价值观

这在具有不同国籍或背景的团体和组织中尤其重要，比如跨国协作和联盟 —— 请注意，很多时候您真的需要跨国合作；在这些团体和组织中存在着不同级别的“专业”（有时反映了社会阶层的结构）。

如果某些团体或成员未被包含在其组织的紧急安全计划中，那么他们可能会将其理解为该组织不太在意他们这些人的安全问题的标志。

例如，您与国际权利组织合作，而该组织没有反映出并计划出在紧急情况下撤离当地合作者（也就是您），而只关注其国际员工。这可以传达一个信息，即某些员工的福祉比其他员工的福祉更有价值。

此外，如果一个组织经常忽略管理人员、清洁工等成员的安全意识的重要性，也会暴露出不专业和不可靠的信号。比如考虑平时谁会接电话，这样的人最容易遇到紧急电话；或者，谁最有可能认识建筑物中的潜在不安全因素？

包容性的方法不仅可以使团队中的安全措施具有更大的凝聚力和所有权，还可以提高每个人的安全水平。

2、恐惧、紧张和不信任

采取新的安全措施还可能会被理解为缺乏信任，即便您真的是好意。

例如，您选择了Utopia从而放弃了您的队友A提议的telegram；如果队友A对 telegram 为什么不安全缺乏足够的了解，您对安全措施的这一更改就有可能被队友A理解为这是对TA本人的不信任。

同样，在某些危险的活动中不易获得情报 —— 您必须采取保密分级措施，这对行动本身来说非常有益；但是这样做也会导致其他活动家之间的不信任感增加，“为什么他能得到这些信息，而不是我？”，人们会这样去想。

也就是说，您制定的保密分级必须合理，并且需要所有参与者认同，以避免这样的误会。

非常建议您以坦诚、开放和诚实的方式简单阐明您采取新安全措施的原因、及其背后的逻辑，这非常重要。听取周围人的反馈和评论，以查看是否有可以避免或解决的后果，并尽一切努力保持双向信任。

另一方面，如果全面地根本性地采取新的安全措施，有可能引起您的对手或中立方的警觉（例如完全转向加密通信和**Tor**，可能引起互联网服务提供商的注意，他们可能会将此信息提交给镇压机构），这种情况下您可以考虑同时使用旧方法、与新方法并行，以降低怀疑。比如，互联网服务提供商看到您 “依旧在微信上活动”，他们就不会想到事实上您已经将所有主要的交互都转移到wire了。其他同理。

采用新的安全措施并不意味着缺乏信任，但人们可能会这样去理解，打破怀疑的办法就是，您必须明确新措施的原因和背后的逻辑。

3、资源的使用

任何可用于提高安全性的资源 —— 如 计算机硬件或软件、培训机会、车辆、获得心理协助和社会支持的机会等等，都应该被负责任地使用。

您需要保持没有人享受特权以优先使用此类资。如果小组或组织内部没有共享资源的整体大目标，那么资源就会被人们用于他们自己的个人利益。这种排他性可以发出这样的信息，即：控制资源的人可以将其用于自己的目的，而无需追究责任。这种影响将对您的组织工作非常不利。

资源是很重要的东西，您需要保证它的分配和使用不要造成分歧。

4、文化特征

文化是其他人用来解释我们的行为的 “镜头”。在多元文化的环境中，最好能考虑如何通过此 “镜头” 来解释新的安全做法。在跨文化协作的环境中，诸如隐私、某些资源、或社会传统价值观、或决策手段之类的概念在不同文化之间通常差异很大。

您需要对您的文化环境保持敏感，并检查您所采取的新安全措施是否可以以避免引起冒犯或分裂的方式进行解释。

为了在您自己的安全性实践中分析您的行为和消息，绘制表格并在自己填写之前考虑给出的示例，可能会很有用。建议您根据这些概念来考虑自己的做法，并与您的朋友、家人和同事在一个安全的空间中谈论这些问题，以努力增强关系方面的积极影响，并减少其消极影响。

上述步骤帮助您为自己定义安全性、并在组织内部创建安全空间，通过对安全状况进行分析和诊断，以及在此过程中计划、维护和改善安全性，规划出一条路径，帮助敏感人士的工作更顺利进行。

如何实施这一系列理想的步骤在很大程度上取决于您的工作性质以及与您一起工作的人的性质。重要的是要记住，它们代表着一个周期性的演变过程，不断评估您的状况以及更新策略和计划，是最理想的。

本集中讨论的是组织的安全能力建设过程的管理，下一步是要了解可以在工作的各个方面实践以提高安全性的特定工具和策略。 这些工具和策略用于特别是敏感人士从事的高风险活动中。

[image]

抗议活动：准备，分析和计划

集会和言论自由应该是每个人都可以行使的基本人权。它们维护了您为自己的信仰进行抗议的权利。然而，很多时候这会带来风险，甚至严重的人身威胁；对这些风险进行规划和做出准备将有助于您保持安全。

只有您能保持基本安全，您的反抗才有可持续性。

各国关于抗议活动的规则和条例各不相同，因此，请确保您了解这些权利是什么，以及现有的限制可能对您产生的影响。

您的言论自由和和平集会的权利受到《世界人权宣言》第十九条和第二十条以及《公民权利和政治权利国际公约》第十九条和第二十一条等的保护。

但是，尽管有国际法的保护，镇压和抓捕依旧非常普遍，作为敏感人士，您必须对此加强认识并采取行动。在我们的 列表-5 中查看 “维稳面面观” 板块，它汇总了最新出现的维稳战术。

接下来的指南将帮助您参与分析并学习一些策略，以便在行使您的基本权利时保持安全。

做好准备

虽然有时您可能会决定自发地进行抗议，但事先认真规划行动是确保您在抗议过程中的安全保障的更好方法。仔细的准备可以防止一些紧急情况的发生，提高您应对威胁的能力。与朋友和同事进行公开、信任的沟通和安全规划，有助于抗议活动本身的安全和成功。

请考虑以下问题：

- 这次抗议的性质是什么，它希望达到什么目的？
- 在这个确切的时刻，这个抗议活动是否是实现这些目标的最有效方式？
- 您如何确保抗议活动的战术默契满足预期，如何控制潜在的渗透者煽动不必要的暴力？

如果您确信抗议是一个好主意，那么开放性地考虑您的安全问题是很重要的 —— 最好是和您的整个团队一起考虑。

在敏感人士群体中，作为一个团体来讨论安全问题可能会有可见的困难。安全问题往往是一个非常个人化的问题，在一些激进团体的文化中，冒险被视为勇敢和善良，而恐惧、痛苦和悲伤被视为弱点。您需要在不违背这种激情文化的基础上，理智冷静地谈论防御措施。

☕

要想共同建立长久的、包容性的行动主义和反抗运动，活动家们就必须接受自我照护、相互照护。在抗议活动前和抗议活动期间，最好能创造专门的时间，以轻松舒适的方式思考安全规划。这应该是一个包容性的和非暴力的空间，每个人都可以在受支持的氛围中一起分享自己的恐惧、并设计防御计划。

对安全采取整体方法，首先需要认识到安全是一个个人的和主观的概念，它取决于每个人自身的情况：因此，您必须重新提出这一概念，并找到适合您自己的定义。您还需要将自我照护、健康和数字安全确立为根本。

即使这是您第一次对安全采取组织化的方法，也并非意味着从头开始这个过程，每个人在这方面都或多或少有一些基础；所以您不必担心学习它的压力。此外，每个人对安全的看法都不一样，在组织团队中，您需要意识到这点。培养和保持对安全状况的健康认识是安全战

略成功的关键。

相关详细做法请参见本教程第1集。

[image]

了解所有行为者

为了制定安全计划，您需要知道谁在保护您，您可以与谁合作，以及谁可以帮助您保持安全。

一旦您有时间和您的团队一起思考和讨论安全问题，您就应该开始一个分析过程，以便制定决策。要考虑的最重要因素之一是谁是：谁是您的盟友和对手。如果您担心您的安全问题，您应该考虑是谁在试图阻止您参加抗议，以及他们通常是如何做到这一点的。他们的策略是什么？

了解维稳当局或非国家团体的哪些人员会出现在抗议现场，以及他们通常采用什么策略以压制您的抗议行动，将有助于您做好准备，以您自身的基础条件作为基准。

您有什么办法可以让警察或其他维稳机构接受您的合法抗议，或阻止他们对您的攻击吗？还是说，你们只需要努力保护自己？您还应该考虑您的盟友，如其他民间社会、外交实体或人权组织，他们可能会帮助您。以及，您有什么医疗支持或法律支持吗，在抗议之前或抗议期间如何联系他们？将这些团体纳入您的计划中，以便他们能够在出现问题时及时支援您。

相关详细做法请参见本教程第3集。

分析风险

对风险的分析应有助于您确定和思考您在抗议活动中可能面临的威

胁，以便您能采取正确的安全措施避免或防止这些威胁，或将其影响降到最低。

常见的对抗议活动的威胁可能包括使抗议活动“非法化”，或对抗议者使用催泪瓦斯榴弹或其他武器。关于镇压者会怎么做，这样的信息非常重要，这就是为什么我们将收集镇压战术的内容板块“维稳面面观”放在列表-5 “直接行动” 中。

把您可能面临的所有威胁列出来，并把它们按优先顺序排列 —— 就是您所认为的严重程度，最严重的那个列为优先考虑。

- 哪些威胁最有可能发生？
- 哪些威胁的影响最大？

一旦您确定了最有可能和/或影响较大的威胁，您就可以考虑如何降低其概率或对您和组织的影响。这可能包括与他人合作，或采取您自己的措施来保护自己。当然，您首先应该知道可以和谁合作，也就是您在前文中的练习里构建的“行为者图谱”。

如果您很匆忙或压力很大，将很难进行这样的风险分析。无论您对事业有多大的热情，在计划参与时，关键是您要有正确的心态。所以，您在前文中构建的心理检测图表，需要时刻发挥作用。

一定要和朋友们确认一下自己的观念，利用一切可以利用的信息，这样才能权衡风险。尽量不要夸大或降低风险。

✓

您应该在每次抗议前进行风险分析，并考虑在两次抗议之间改变您的策略，以免令您的防御策略对镇压者来说“可预测”。

明确计划

根据您的分析，您应该与您的朋友或其他参与抗议活动的同伴一起制定一个明确的行动计划。该计划应该包括您为减少您所发现的威胁的可能性所做的一切，以及制定一个“B计划”—— 您在紧急情况下为减少其影响而采取的行动。

您不一定要写下每一项计划，但 它们应该是明确的、详细的，并得到每个人的同意 。

花点时间看看地图，熟悉预期的行进路线或静态抗议的位置。确定医院、警察局和其他资源都在哪，并与您的朋友商定集合点和疏散路线。

您的计划还应该包括安全通信和使用数码设备的策略，以及如何在抗议活动结束后和万一出现问题时，相互照顾和保持安全的方法。相关知识可参见我们的 列表-5 “护盾” 板块。

在示威活动中，想象力、创造力和幽默感要有效得多 —— 请参见我们的列表-5 中的板块 “技巧、策略和原理”。本项目将在未来开设专题站点讲述战术问题。

✓

请记住，如果您没有计划，您就必然会成为别人的计划的一部分。

有关如何制定安全计划的更多信息，请参见本教程第7集的内容。

在下一集中，我们将开始进入您的行动主义组织内部的关系构建技巧，只有当你们能互相支援、互相依仗时，所有人才能获得安全，您的行动才有获胜的机会。

[image]
[image]

您需要真正的“自己人”：整体安全S01E09 - 进入战斗状态

[image] 关键词	亲密团队 准备工作
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年4月7日
[image] **Description**	教材

您身上的东西既可以在预防或应对攻击或事故时非常有用，也可以被用作骚扰您的借口。

- Table of Contents

  创建一个亲密团队
  维护您的心理健康
  构建包容性的运动
  进入抗议行动，第一步：考虑带什么
  不要带什么 ——
  需要带什么 ——
  做好被搜查的准备

欢迎回来！

本集内容将进入您的行动组织内部的关系构建，然后开启行动。只有当你们能够互相支援、互相依仗时，所有人才能获得安全，您的行动才有获胜的机会。

关于什么是支援和依仗，还记得我们举过的枪战的例子吗？您非常有

必要找到那样的感觉。

为了更有效地和安全地进行抗议，您就非常有必要与一群朋友或同事进行协调，以便共同行动和相互照顾。这是需要技巧的。在这里，我们考虑一些有用的策略来协调您的行动，以保证您自己和他人的安全。

[image] [image]

创建一个亲密团队

亲密团队是由抗议者同伴或朋友组成的小团体，大家一起准备、执行行动，并且，作为一个“单位”与更大规模的行动/运动项目互动。

他们共同制定安全计划，并对行动和紧急情况下的反应进行分工。亲密团队通常由2～15人组成，即 规模小到可以让成员之间进行个人分享、直接信任和关怀。

这样的小团体可以为某项特别的活动（如非暴力行动、抗议、示威）而成立，也可以成为一项大型运动的连续组成部分。它们可以是自主的，也可以由其成员分别组成一个更大的团体。

如果您成立了一个亲密团队，请考虑首先决定每个人各自的角色（如协调员、代表、媒体联络人、医疗支持、“观察员”等等，基于每个人的性格特征和专长，并建立一个决策结构。

每个人都会在决策中发挥作用，所有人的共同协作就能让一项任务顺利和完美。

重要的是，您的亲密团队在行动中要保持密切沟通，共同应对紧急情况，并一起撤离。

所有成员花时间一起规划行动，检查彼此对安全问题的看法。行动结

束后，最好一起离开并进行汇报。理想的情况是，团队中的一两个成员应具备在紧急情况下进行急救和心理互助的能力。这很重要！

维护您的心理健康

如果您希望自己的行动具备可持续性，就必须首先学会照护自己和队友。随着时间的推移，压力、疲劳和创伤都是任何活动家面对的最大威胁，有很多活动家往往在还没有直面维稳当局的时候，就被自己的心理压力击垮了。

这就是为什么心理健康必须是整体安全的一个重要部分之一。保持您的健康并不是为了宠爱自己；事实上自我照护本身就是激进的、是政治的，对于应对创伤、愤世嫉俗和倦怠等威胁至关重要。

抵抗现行体制在人们身体和心理上的作用是很困难的。所以在您开始行动之前，请考虑以下问题：

1、当您达到一个不健康的压力水平时，您的身体状态和心理状态倾向于如何做出反应？还记得您在前面教程中构建的压力测量表吗，现在就用它来监测您自己的健康状态。

找出哪些做法或资源有助于帮助您的身心恢复到健康状态，以及如何将它们融入到您的反抗行动中。

2、在您的亲密团队中培养一种文化，在这种文化中，您可以分享自己的恐惧，公开谈论压力和创伤经历，而不会担心被误解和嘲笑。

这也许不是容易的，反抗团体有一种根深蒂固的且普遍的内部文化，即 将恐惧和压力视为懦弱和无能，甚至可疑。这导致人们不得不隐藏自己的真实心态，原本可以建立知心关系从而实现更默契协作的队友之间，因此而产生心理隔膜。

中文里面有一句话说的很好，“一万句我爱你，不如一句我懂你”，互相理解是活动家团队之间构建亲和力的最佳途径。

3、练习积极的倾听，建立团结和相互关怀。

这不是简单说说的，因为并不容易做到。任何团体都会受到其成员所在的社会环境的影响，反抗团体也一样；如果您所在的社会是人情淡薄的、物质主义的、互相利用的人际关系，您就想需要警惕这些东西被带入到您的行动主义团队中。

✂

行动者的成功永远不会是个人成功，对于行动者来说只有好的团体协作才能获得真正的成功；所以您知道，在争执中占上风并不会给您带来任何荣誉感，它只会让您失去队友的支持，从而失去获得真正成功的机会。

积极的倾听是技术，而不仅仅是态度，您可以在这里看到更多解释。这需要练习才能做到，尤其是在社交媒体与真实生活之间的界限越来越模糊的当下时代，社交媒体上的偏执和变态的超个人主义已经在侵蚀现实生活中最重要的福祉来源。行动者必须警惕这点，并主动培育积极的倾听。

正如您在我们的另一个系列“行动主义”第2集中看到的，当权者也必须紧密团结其各种支柱机构，才能维护权力稳固；如果反抗者不能做到更团结彼此，你们将难以击败那些齐心合力镇压你们的权势。

4、在抗议活动期间，确保您有足够的食物和水，并为不同的天气条件做好准备。下一集中将对此有更多细节。

5、抗议结束后，确保在到达安全地点后，花时间与您的亲密团队进行汇报。这也非常重要。您将在后面的教程中看到更多对此的介绍。

6、腾出时间与您的团队进行必要的分享和互相支援，但也要花一些时间独处，以处理这段经历，并回归您的日常生活。

“完整” 对任何一种行动来说都很重要，就如科学的作息时间能帮助维护您的健康那样，反抗行动也有其科学的节奏，如果您希望自己在每一次出击时都能有焕然一新的精神状态、能发挥自己最好的水平，您就有必要在日常照护好自己。

构建包容性的运动

当我们谈论安全时，我们不仅仅是在谈论保护自己不受催泪瓦斯的伤害。对我们许多人来说，安全感来自归属感、团结和相互尊重，特别是在人们可能因性别认同、种族、性取向、外表、或其他因素而受到歧视甚至遭受暴力的情况下。

如果您是受歧视较少的人，或享有较多特权的人，可能甚至没有注意到，当您计划或实际参加抗议活动时，您正在用自己的行动复制您的特权，并助长边缘化。在您的运动中，有多少有影响力的职位是由来自传统特权群体的人所占据的（比如异性恋男性、社会上的中高阶层、名人）？因性别认同、种族、宗教、性取向、经济地位、社会地位或教育地位、或其他类似因素而继承的特权和相应的歧视，往往是不公正的产物。

如果您要与社会上的不公正现象作斗争，您就必须首先在自己的人权运动中与这些现象作斗争。

花时间仔细看看您的团队，考虑一下您是否需要在这些线上更平等地分配责任。如果团队中的一部分人似乎拥有所有的权力，那么就要对此提出挑战。

考虑给人们一些机会，让他们因自己的身份而在社会上被剥夺的机会，能够在您的亲密团队中重新获得。

在您的运动中，对任何歧视、性骚扰或暴力都应该是零容忍的。明确指出，任何从事这些行为的人都将受到惩罚，或可能因此被从运动中

除名。

这些问题决不是一个“轻松”的玩笑素材。要知道，面临歧视的人可能也需要特别的保护措施，或者在抗议活动中更积极地融入。在制定安全计划时您需要提出这个问题，并根据这个问题考虑您的行动策略。

进入抗议行动，第一步：考虑带什么

重要的是要认真思考 —— 您要带什么去参加抗议活动。请记得，您身上的东西既可以在预防或应对攻击或事故时非常有用，也可以被用作骚扰您的借口。

您应该已经在前几集的练习中进行了充分的背景和风险分析后，才考虑要带什么东西。您需要与您的亲密团队进行协调，根据每个人的责任分配资源。

虽然每一种情况都是独特的，但下面的说明性清单可能会有帮助：

不要带什么 ——

1、如果您不完全清楚电子设备上有什么，就不要带电子设备。

自从有智能手机的那一天开始，它就被用于镇压抗议者了，直到如今。镇压者对智能手机的利用一直在不断快速提升，事实上您很可能无法做到完全“清楚”地知道当权者会如何借助您的手机来对付您，直到黑客将警察的秘密文件公之于众。

所以，理性的建议应该是不要携带智能手机，但很多时候在抗议现场

的人需要记录现场状况，对警察的暴力行为取证，并且行动主义团队需要彼此间保持联络，有手机会更方便。

总之您必须根据自己的具体情况进行权衡，您的选择必须能让收益高过风险，您愿意为收益承担风险，尤其是，您需要明确知道该如何减轻和避免风险。

对此的更详细内容请参见本站的“行动安全性”栏目。

2、尽可能不要携带任何可能给您带来麻烦的东西：任何可能被认为是武器的东西，或任何非法药物或酒精。

总之，镇压者会努力寻找把柄以控制您，不要给他们制造机会。如果必须携带，请事先准备好稳妥的撤离方案。

需要带什么 ——

1、携带您需要的特殊药物 —— 不是管控药品！是能帮助您维护健康状况的必要药物。

抗议活动现场理论上应该有医疗团队，但他们携带的药物和急救工具往往倾向于医治暴力冲突导致的创伤；如果您有慢性病，他们的急救箱里不一定有适合您的药物。您应该自己携带。

2、一些现金，以备不时之需 —— 是现金，而不是银行卡和在线支付账户！能识别您的手机的人就能冻结您的账户，这是一种威胁抗议者妥协的常用方法。如果您有现金，就不需要担心这样的状况。

您往往不会知道一场抗议活动会持续多久，有现金在身上会很方便。

3、舒适的衣服，让您可以轻松活动的款式 —— 不论您的抗议活动是否完全和平非暴力，您都应该为镇压做好准备。为您的应激反应动作

做好准备，随时可以奔跑、攀爬、躲闪，衣服和鞋子的选择很重要。

4、如果您需要带手机，可以考虑换一张新的没有实名的SIM卡，或者新的一次性手机。记得提前充值通话时间，并携带一个移动充电器。

5、紧急联系人：考虑将最重要的联系人写在手臂或腿上 —— 是写在自己身上！而不是放在手机里。您的手机可能丢失、可能被警察抢走、可能没电和摔坏，您不应该把最重要的东西放在手机里面。

您的紧急联系人应该是您最信任的人和最可能需要的人，比如律师、亲属、队友，您肯定知道您需要谁。

6、急救和卫生：小型急救箱、卫生纸和卫生巾 —— 可以帮助您自己处理简单的伤势，也可以帮助身边人。一个团队中只需要一个人携带急救和卫生用品即可，但是，其他人需要知道如何随时联系到这个人，不要走散。

7、食物和水 —— 带一些高能量的体积小的食物，巧克力或者压缩饼干、能量棒等，以及紧急情况下既能饮用又能清洗伤口的洁净水。带上足够的物资，以备万一有什么变故，您也能维持比计划中的抗议时间更长的时间。

8、带上泳镜/护目镜、围巾、面罩 —— 以抵制催泪瓦斯，携带一些治疗催泪瓦斯引起的烧伤的抗酸溶液。

比如抗酸药（例如美乐事）水溶液可以对抗催泪弹造成的烧伤，或者稀释过的抗酸药和碳酸氢钠水溶液。在遇到催泪瓦斯时，首先要做的就是尽快远离，躲避到通风良好、有新鲜空气的地方；由于比空气重的CS气体会往下沉，因此不要蹲在地上。要快速跑起来。

9、考虑携带一个小型相机，用以记录警察的暴行 —— 您的团队中最好可以安排特定的接受过这方面专业训练的队友负责拍摄记录。如前所述，您的亲密团队已经在行动之前做好了明确分工，并且每个人之间都知道彼此的角色，以及在什么时候如何与最需要的队友协作。

10、在一些国家，没有携带身份证件可能会成为逮捕的借口，但在其他国家，没有义务携带身份证件，甚至身份证件可能会被警察用来对付你。与您的亲密团队协调是否要带身份证件，如果要带，带哪种。

做好被搜查的准备

在许多情况下，镇压当局拦截和搜查抗议者是一种很常见的做法，他们声称防止将武器或其他非法物品(如酒精或毒品)带到抗议现场。然而，这也常常被用作对抗议者进行恐吓和骚扰的借口。

很可能有既定的行为准则来规范警察可以如何搜查你。请咨询相关律师，了解警方在此面临的法律约束，以及每种情况下的实践现实。了解您的权利。

准备并练习任何应对搜查的口头抵抗（如果在某些情况下可以抵抗的话），并确保您没有携带任何非法物品。并且，如果遇到被搜查的情况，要告诉您的团队，让大家提高警惕。

[image]
[image]

协调性很重要，从场内到场外：整体安全 S01E10 - 安全是保持战斗力的绝对必要条件

[image] 关键词	团队 安全文化 通信
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年4月8日
[image] **Description**	教材

拒绝所有那些试图将安全技能和“缺乏勇气”联系在一起的论调，他们是骗子。勇气从来都不是愚蠢和盲目的，如果您希望自己的行动可持续并取得成效，安全技能就是您必不可少的武器。

- Table of Contents
在抗议行动的过程中：经常和安全地沟通

欢迎回来！

从现在开始，进入行动部分。

[image]

许多人权维护者和活动家严重依赖电脑和手机来组织和协调和平抗议活动。然而，这使得没收、盗窃、和监视您的电子设备和通信能力成为了试图限制言论和集会自由的镇压者的“优先事项”。

虽然在某些情况下，透明度和与国家和社会的公开接触可以是有益的安全工具，但是，在更多情况下，保护抗议参与者的身份信息和敏感通信信息是非常重要的，至少在某段重点时间内是如此。

如果您正在计划或协调通过互联网或使用手机进行动员和联络的抗议活动，您应该考虑如何保护您自己和您的团队的身份。这与您的 “勇气” 无关，而是将决定您的运动的可持续性和成效。

有时，当局或其他人会对社会运动进行密切的监控，以预测、防止或破坏任何抗议活动。政府和私人公司使用窥探、渗透、和自动搜索等战术，利用特定的文字或图像信息识别社交网络中的用户，以及人们之间的关系，不仅能定点打击，还能连锅端。

因此，依靠社交媒体来组织抗议活动是很危险的，因为通常会受到严密的监视。您至少需要首先衡量自己的情况，以匹配基本保护措施。

在组织或参与行动时，您可能希望避免在社交网络上使用自己的真实姓名、避免与可能受到社交媒体网站监视的团体有关联、避免接受 “好友请求” 和其他与您以前不认识的抗议者的联系。考虑使用VPN或Tor浏览器，隐藏您的IP地址和浏览活动。具体做法可参见“行动安全性”部分。

在抗议活动中，您的对手会使用他们拥有的一切技术能力，以查明抗议参与者的身份，因为他们想要抓捕 “价值最高的人”，也就是一场行动中影响力最大的人，以便镇压当局可以以最快速度瓦解整场运动。

要做到这点，镇压当局就需要尽可能知道所有参与者的身份，以及参与者之间的关系网络和关系强弱度。这是他们的战术。而您的战术就是，尽可能阻止他们对您的了解，至少是在此给他们加大难度。

要做到这点，首先就要做到知己知彼，还记得本系列最初部分做过的练习吗 —— 了解对手、了解自己、了解地形。作为例子，可以在这里看到镇压当局将采取哪些技术能力：《警察用哪些监视方式瞄准抗议者？》，尤其是《如何识别抗议活动中可见的和不可见的监视》。

您可以在我们的 列表-5 “护盾” 中看到提供给行动者的保护性措施，并在同一列表的 “维稳面面观” 中看到您很有可能面临哪些形式的镇压手段 —— 即 了解对手，和了解自己。

如今全世界的活动家都知道在上场之前需要先遮住脸，但这绝非全部；您可以在上述内容中看到，镇压手段从在线到线下，丰富多样。事实上仅仅遮住脸部是没有意义的，对防御来说，如果您想让您的战术起效，您就需要至少和镇压者的思考范围一样地全面。

不过，遮住脸部可以成为一种非常不错的运动符号，比如占领运动期间使用的 “V-for-Vendetta” 面具，以及俄罗斯的 Pussy Riot 和墨西哥的 Zapatista 运动等团体使用的象征性头巾。

面具/面罩可以用来为活动家团体创造一个象征性的身份，或者代表那些不能参与抗议的人。需要注意的是：在许多国家，在抗议活动中遮住自己的脸是非法的，有可能成为逮捕您的借口。在决定这样做之前，一定要确认您所在国家或地区的法律情况，在此处重复前文中的练习，与您的团队协商以确定具体风险和你们的承受能力。

还有一点需要注意！如果您的面具/面罩太过普遍，也就是说，很容易可以买到或得到，您就需要小心渗透者可能佩戴同样的面具/面罩，以暴力恶性行为污染您的运动。由于媒体非常倾向于聚焦刺激性的行为和事件，于是，如果渗透者采取暴力故意违反您的运动准则，他们而不是你们，更容易被媒体捕捉，并放大负面影响，从而动摇您的运动的支柱。

这些都是您需要在行动策划阶段考虑到的问题，对此您可以采取一些预防措施 —— 比如提前注册一个运动 “官方” 社交媒体账户和网站，严格管理这些信息窗口的权限！编辑权限一定要完全掌握在自己人手里。一旦遇到渗透，您的组织可以快速通过这些窗口纠正媒体的错误。不论暴力恶性行为是什么人实施的，您需要迅速声明切割实施者，不要令其被作为您的运动的一部分。

还记得上一集中构建的亲密团队吗？您已经为每个人分配了角色，其中就包括媒体联络人；在这里启用这个角色。

[image]

如今几乎任何防御安全建议都会告诉行动者：不要携带自己的手机。因为您的手机可能被警察抢走、被盗、在冲突中丢失，尤其是，您的手机是比您的身份证更详尽的关于您的一切的档案馆，如果警察想要构陷您，将轻而易举。记得红衣教主 Cardinal Richelieu 的名言：“给我这个世界上最诚实的人写的六行字，我一定能从中找到足够的理由来绞死他”。

手机对联络来说非常重要且方便，您需要与您的队友保持联系、及时协调，于是安全建议会告诉您，携带一部与您的身份完全无关的一次性手机。具体方案见《买不起/买不到一次性手机怎么办？这里是您在参加敏感行动/之前需要了解的事》。

如您所知，如今的镇压战术不仅在抗议活动现场实施，当权者已经不满足于这点了；他们想要在抗议活动开始酝酿形成的阶段进行扼杀，即 所谓的 “预测性警务”。

所以，对于行动者来说，您的防御战术不仅需要在具体的行动过程中，而是，在开始动员的最初就应该严密部署并有效实践。

[image]

在抗议行动的过程中：经常和安全地沟通

为了抗议活动的成功，您的团队各成员之间最好制定一个明确的沟通计划，以监控事态发展、协调行动和应对紧急情况。

此前您已经为队友分配了角色，每个人都明确知道自己负责哪一个部分，其他人也能知道和记住在遇到哪种情况下该联系哪位和哪些队友。

比如，如果有人受伤了，您不仅需要联系负责紧急医疗救助的队友，

而且需要联系负责记录真相的队友，将整个过程拍摄下来；再比如，当你们中有人被捕了，其他人应该迅速知道这件事，并知道被捕的队友负责的工作需要由谁来接替 …… 设置好一套规则，把所有可能性都尽可能考虑进去，确保你们所有人都了解并记住内容。

由于您可能需要处理突发事件，因此，明确在特定情况下与谁联系、何时联系、如何联系都是很有帮助的。

您或您的亲密团体的成员之间还应该与抗议活动之外的联系人保持定期沟通，以便他们在出事时能够发出警报，比如亲人、律师、可靠的朋友、可靠的国际权利组织等。

尤其是负责记录真相的队友，应该尽可能确保万一自己被捕，拍摄记录的内容也有一个安全的备份 —— 不是在云端！而是在您的亲信手中，而警察不应该知道那个人是谁。

安排时间与您的紧急联系人联系，分享安全指标，并商定：如果出了问题，你们会怎么做。如有必要，可通过民间社会组织和人权团体来进行。

列出一份在紧急情况下可以联系的人和组织（包括律师等）的名单。如果您不得不将此名单保存在手机上，可以考虑使用代号/昵称来标记它们，而不是真名和身份。不使用手机号的安全通信应用是最好的，每个人都使用昵称显示，而只有您知道每个联系人都是谁。

也要随身携带一份书面副本，以防手机丢失、决定不带手机、电池或通话时间用完等等状况。尤其推荐把最重要的号码写在胳膊或腿上。最好编辑一下该号码！不要写出完整的手机号码，不要让警察看懂，而您自己应该可以看懂。

确定替代的通信手段：不要完全依靠个人设备来沟通 —— 有时公用电话可能是保持联系的唯一选择。甚至是风筝、彩色烟雾等等 …… 发挥您的创意。

不要使用移动电话、短信、和没有端对端加密的通信应用，它们都很

容易被窃听，而且在抗议期间，这种通信渠道被当局或其他对手监视的情况越来越常见，所以要牢记这一点。

除热门安全工具外，还可以在本站的“工具”栏目中找到您需要的解决方案。

有时，创建和使用自己的隐语可能是一个非常有效的替代方案，还记得新疆的异议人士是如何做的吗？在这里看到《维族妇女对战中国的监视国家》。

您需要确保在抗议活动开启之前让您的队友练习使用所有安全工具和应用程序，以便你们知道如何识别它们是否失败、并选好可能的替代方案。

演习是个好办法。

下一集中我们将继续更新抗议活动过程中的注意事项，包括技巧提示；您不会知道什么时候能 “起风”，但我们应该能做到，在风来之时，我们的帆已经坚固地撑起来。

[image]
[image]

抗议中谨防常见危险：整体安全 S01E11 - 协作和互助就是战斗力

[image] 关键词	人际安全 团队 行动
[image] 关联	[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2025年4月9日
[image] **Description**	教材

如果您正在培训中实践这套教程，将其中关联的所有文章作为知识点加入您的课程。

- Table of Contents
安全记录抗议现场，并安全发布
在点击记录和分享之前，请考虑以下几点：
抗议中：谨防常见危险
监测事态和共享安全指标
照顾身边的抗议者

欢迎回来！

本集继续描述前线。

[image]

安全记录抗议现场，并安全发布

如果您在抗议或示威活动中目睹了侵犯人权的行为（经常会遇到的）您可能想做的第一件事就是拿起自己的手机或相机把具体事件记录下来，然后在网上分享，或保存起来以供日后作为问责的证据。

但是，如果您不够小心，记录和分享侵权行为可能会让您或其他队友陷入困境，所以，您需要一些技巧。这点也是我们曾经重点关注的技能之一；如果您正在进行培训，请将本站“行动安全性”中的相关内容列入教程。

在点击记录和分享之前，请考虑以下几点：

首先，在您开始拍照或录像之前，要确保您自己在一个尽可能安全的空间里。理想的情况是，在您拍摄时有另一位队友负责拍摄您。反之亦然。以防您成为警察或对手攻击或骚扰的目标。

这种策略可以事先与您的亲密团队计划好。

如果您使用的是智能手机，有很多方法可以安全地拍摄照片或视频。

比如，Obscuracam 可以让您模糊脸部，以防止现场活动家的身份被警察的社交媒体情报所识别； CameraV 可以让您控制图像或视频中的元数据。

EyeWitness to Atrocities 应用程序可让您记录可合法核实的镜头和图像，可以作为证据提交给法庭；Mobile Martus 则是专门为记录侵犯人权行为而设计的。

Mobile Martus 还允许加密传输信息，您可以在线上传内容，同时使用 Orbot 保护您的身份。

发送文件时，请避免使用未加密的彩信。考虑使用像 Signal 这样的端到端加密通信应用，或者GPG加密邮件。

如果您把内容存储在SD卡上，可以考虑对手机进行加密，或者让卡“跑路” —— 采取接力的形式把它交给您信任的队友，由队友把它带到安全的地方。

如果您在活动中记录了任何侵犯人权行为，现在想直接发布或分享，您可能需要采取一些具体措施来保护您的身份和图片或视频中其他人的身份。

图片和视频包含EXIF数据，这是一种元数据，可以识别图片的拍摄地点、时间，甚至是由谁拍摄的。您可以使用工具删除这些元数据。在本站“工具”栏目中找到。

尤其是，使用这些工具必须具备战略性，因为根据不同情况，有些时候您可能需要保留元数据，以将此信息作为可供法庭采用的证据。

比如 CameraV 还可以用来为图片或视频添加额外的元数据，这对信息验证来说非常有用。

当上传或分享材料时，通过使用Tor浏览器（或Android智能手机的Orbot）或加密的VPN服务来掩盖您的踪迹。

如果您担心分享您所收集的信息的安全性和法律影响，请向律师和人权组织寻求专家建议和支持。确保保存安全的备份！并考虑是否保存非匿名的资料 —— 如果是，如何保存。

抗议中：谨防常见危险

在抗议活动中，镇压者有一些常见的战术经常被用来对付活动家，所以了解镇压手段很重要，您在制定自己的战术时需要针对这套镇压手段做好准备。

镇压者的战术是有规则的，关于警用武力和相对应的防御工具可参见

本站“行动安全性”部分教程，以便帮助您通过观察镇压部队的布局，就能预测到他们将采取哪种战术。

但警察和镇压部队的冷热兵器还不是抗议者面对的全部威胁，监视技术、心理战、信息战等，都需要被作为具体的威胁模型加入您的战术策划中予以分析。在我们的列表-5中看到具体分析和防御方法。

您也可以观察任何可能对抗议活动构成威胁的个人的行动，比如疑似的渗透者，并与您的亲密团队或更广泛的抗议活动同盟分享您观察到的迹象—— 例如他们行为的发生了变化。

可疑渗透者行为的变化往往是暴力镇压的前奏，相关内容请参见本站的主题栏目。

除此外还要注意：在抗议活动还在进行的过程中并不需要专注于阻止渗透，而是应该专注于防止渗透所引发的危险—— 尤其是当渗透者显示出暴力袭击他人的倾向时，那就是镇压部队暴力出击的预兆。您应该尽可能保护自己和队友的安全，揭露渗透是事后的工作。

催泪瓦斯是特别常见的 “人群控制” 武器，并越来越多地用于扼杀抗议活动。然而，催泪瓦斯中使用的化学品类型在不断变化，这意味着有效的补救措施也必须变化—— 您在网上搜到的防御方法不可能一直确保有效。您可以在本站的“行动安全性”中查看详细内容。

活动家应该试着找出您所在地区的当局使用的催泪瓦斯是哪种类型的。如果您能得到一个防毒面具，会有所帮助，但是要避免使用旧的，因为它们本身可能是有害的。

泳镜可以帮助保护眼睛，但如果受到催泪瓦斯的影响，用水稀释后的抗酸剂或敌腐特灵溶液(一种针对化学品飞溅的急救产品) 可能会有帮助。

水炮也是非常常用的暴力对付抗议者的工具。在近距离的情况下，这

些水炮可能非常危险，所以，如果你看到警察要在你附近使用水炮，请尽快离开。

此外，中国不知道有没有骑警，在欧洲，骑警出现在抗议现场是比较常见的。这种马喜怒无常，被它们踢到有可能严重受伤。所以您应该避免从后面接近马匹，更不要直接站在或蹲在马匹前方。

监测事态和共享安全指标

抗议活动中的安全形势可能会很快发生变化。分享和分析您注意到的任何可能影响您安全的异常情况都是很重要的。这些指标—— 有时被称为 “安全事件”—— 可以帮助您尽早做出决定，避免直面威胁。

尽量时刻保持对周围情况的认识和关注。在抗议活动中建立一个安全小组—— 或在您的亲密团队中指定一名安全人员—— 都是很有帮助的，分工协作很重要，专职人员可以专门负责监测任何安全指标，并根据这些指标协调行动。

请注意您的团体内部和外部的指标，例如有人携带武器或非法物质，有人试图使用暴力（他们可能是渗透者），或者有人变得疲劳、疲惫等。同时，观察警察的行为：他们携带什么装备？附近是否有便衣警察？如果您注意到他们，记下他们是谁，观察他们的行为。

当您注意到任何奇怪的事时，可以口头或通过安全的通讯渠道与您的朋友、亲密团队、或抗议活动的组织者分享；然后，您可以分析它是否构成威胁，并在必要时联合采取行动。

关于监测和分析安全指标的具体方法在本教程第5集中。

照顾身边的抗议者

每个人都有参加抗议的平等权利，包括儿童、老人或残疾人。每个希望参与和平抗议的人都应该得到支持和尊重。

然而，虽然抗议对每个人来说都可能是危险的，但由于年龄或能力等具体个人因素，有些人会面临特殊的危险级别和挑战。尤其重要的是，那些有能力的人，要向其他在抗议活动中可能面临更多伤害风险的人提供一切可能的帮助或保护。

确保所有年龄和体型的人都有代表参加有关抗议和安全决策的会议。在实施安全计划时要考虑到他们的需求，并在抗议活动中照顾他们。

也许您可以成立一个小组，负责照顾有特殊需求的抗议者（如视力障碍、听力问题或行动不便的人）。但是，作为组织者您应该避免代替他人做决定：您需要倾听他们的需求，共同设计一个计划。

下一集中我们将讨论管理心理状态的注意事项，不仅包括您自己，也包括您的队友。活动家的心理状态和掌控自己心理状态的能力是很重要的，镇压者往往很擅长观察抗议者的状态，以便趁虚而入；如文中的练习所展示的，压力和恐惧应被视为一种安全漏洞。

[image]
[image]

场内协作和场外接应同样重要：整体安全S01E12 - 紧急撤离和汇报评估

[image]	关键词	协调 压力 团队 心理安全 行动
[image]	关联	[image]S01整体安全 - 总章节：前线安防入门课
[image]	创建时间	2025年4月11日
[image]	**Description**	教材

不要给对手以可乘之机。

- Table of Contents
事先花点时间整理一下您的想法，在您的框架内加入以下问题：
如果您的抗议者同伴被捕，请考虑以下几点：
为了安全，请考虑以下几点：

欢迎回来！

这里将是本套课程的最后一集。

[image]

当团体成员处于压力之下，或感受到恐惧和受到威胁时，就会对集体动态产生负面影响。这样的群体可能会变得更加专制，人们可能会说出和做出伤害对方的事。

您需要避免这种情况。

当您在抗议活动中需要快速做出决定时，恐惧、压力以及它们所导致的人际问题，可能会阻碍您做出恰当决定的能力，使您陷入危险之中。

因此，在进入抗议活动之前，您应该先建立一个清晰的决策结构或共识程序，以及沟通渠道，这是很重要的。决定一套 “不可谈判” 措施 —— 针对给定场景的行动方案，这些方案在行动开始后不会再进行辩论，直接执行（如紧急撤离战略）。

如果必须对某个问题进行辩论，考虑谁需要参与讨论：是整个团队，还是一个工作组？如果辩论中不必要的声音太多，就会成为一种阻碍，它会减缓决策的速度。

辩论时，尽量练习积极倾听，以避免误解，确保每个人都能理解所谈的内容。作为一个过程，可以考虑共识决策法：每个参与者都可以否决一项提案，但否决权只能与反提案一起使用。也就是说，如果没有更好的建议，否决权就不成立。

偶尔，恐惧可以非常有用地帮助我们逃离危险的环境 —— 只是基于一种本能的感觉，认为有什么不对劲。如果您的直觉告诉您正处于危险之中，这种情况下建议您与自己的亲密团队中的某个人分享，并检查您的感知：您所感知的指标是什么，这一指标告诉您有什么不对劲？与您的朋友或亲密团队一起分析，并共同做出决定。

亲密团队应该为分享抗议前后的恐惧和压力影响提供明确的空间。此外，为了放松和管理压力，单独或与亲密团队一起进行愉快的活动是健康的（selfcare）。考虑让您的亲密团队中的一个或多个人负责组织这项活动。

关于恐惧和对威胁的本能响应的更多信息，可以查看本教程的第2集。

在抗议或示威活动中，您经常可能目睹当局或其他反对您的抗议目标的团体的侵犯人权行为。为了协调反应，您必须尽可能准确地报告所发生的事。而当您就是当事人时，很可能会感到害怕或痛苦，这种情况下报告事实可能会非常困难。

为了避免这种情况，您需要在行动前对此拟定一个框架/准则，在您的压力水平正常、足够冷静的情况下确立这个框架，在现场状态下您只需要按照框架的要求去回答问题就可以了，就像做填空题。

在紧急情况下，准确的信息流是至关重要的。确定需要联系的人和优先顺序，优先考虑能够提供有效和即时支持的人。

在试图报告任何事情之前，您必须做的第一件事就是尽量到一个安全的地方；然后，与最有可能在安全空间中的人取得联系 —— 最好是一开始就不在抗议现场内的人。

您应该事先准备好他们的联系方式，非常建议写下来，写在自己身上或确保不会丢失的便条上，如果只放在手机里可能是不够安全的。

手机这类很容易丢失的设备中不要长时间存放任何重要信息。

事先花点时间整理一下您的想法，在您的框架内加入以下问题：

- 你是谁，你在哪里？
- 发生了什么事？

- 在哪里发生的？
- 什么时候发生的？
- 谁受到了影响？
- 谁是肇事者，你怎么知道？
- 你需要什么？
- 如何以及何时能联系到你？

如果您认为某些情况很有可能发生，那么在抗议前练习一下可能会很有帮助。

如果您的抗议者同伴被捕，请考虑以下几点：

1. 记下逮捕的地点和时间，以及有关逮捕官员和任何有关车辆的信息 —— 姓名或警号通常印在警服上，不难识别。这些信息对于在亲密团队、人权组织、和您想要合作的媒体中传播，至关重要。

2. 如果被逮捕的人是您所在的亲密团队的成员，请立刻进行点名，确认其他人都没事。正如我们在安全通信准则中讲述的，您最好能做到定时点名，以便能够及时发现失踪的队友。

3. 确认被拘留者的位置、他或她的身体状况的细节、以及当局对他或她的指控是什么。如果您认为可能会出现被逮捕的情况，您应该在抗议之前制定一个全面的策略，可以有渠道要求立即释放，最好是让本国和/或国际人权组织参与进来。

4. 如果您不希望逮捕事件阻断您的行动，则应进行重新组合，调整计划，必要时重新为每一位队友分配职责。所以，您的战略中需要有

Plan B，把这些可能性及应对措施都加入进去。

具体方案可参见《直接行动分布指南》，这是一份比较详尽的行动中战略建议。

[image]

在抗议活动结束时，或者如果您提前离开，您的第一反应可能是放松，这会导致您分心。镇压者或您的任何对手都可能会利用这个时机来识别和骚扰抗议者，特别是当人们分成小团体或独自离开时。

为了安全，请考虑以下几点：

1. 保持警惕：继续监测您周围的情况，直到可以确定您已经抵达一个更安全的空间。

2. 不要独自离开：至少成双成对地离开，或与您的亲密团队一起离开。

3. 沟通：让抗议活动之外的人知道您要准备离开了，以及他们应该期待您何时到达预定地点。尽量使用安全的通信渠道进行沟通！这样一来如果您没能按照预期时间抵达预期地点，您的联络人应该立刻提高警惕，推测可能出事了。

4. 反监视：如果您觉得自己被跟踪了，不要直接走小路，而是要尽量迷惑跟踪您的人，让他们难以确定您的真实目的地。对此更多见《在你的日常生活中应用隐蔽野战技术》。

5. 不要逗留：不要在抗议活动发生的区域逗留太久。

6. 考虑如何处理材料：横幅、传单和其他材料可能会把您和抗议活动联系起来。尽量安全地处理它们，或将它们打包藏到外人看不见的地方。

7. 照顾好您拍摄的照片和录音或录像：把它们藏在身上，或者在拍摄后立即让一个不显眼的 “慢跑者” 把它们带到安全的地方。

详细做法见本站“行动安全性”专题中的以下内容：

- 《如何安全地留住证据：给真相的记录者一些技术技巧建议》
- 《公民取证技巧：如何留住真相？》
- 《当你手握真相：最基本的防护知识》

最后，一旦您到了一个安全的空间，就和您的亲友团队一起汇报，并尝试花一些时间单独 “过渡” 您的心理状态。这同样很重要，不可能让自己持续处于紧张状态下，如果您希望在下一次行动时能保持同样充沛的精力和活力的话。

《整体安全》基础教程到此结束。感谢学习！

本站所有教材均可进行您所需要的可视化再创作，包括在您的培训工作中进行更深入的本地化处理。如果您发布它们，请注明来自《**iYouPort - Initiatives & Tactics ＜Phase II＞** 整体安全训练营》。

[image]
[image]

S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法

[image] 关键词	个人 中国 低技术性 团队 防御
[image] 关联	[image]镇压应对措施 ；[image]数字技术限制和最佳实践 ；[image]匿名手机
[image] 创建时间	2025年4月12日
[image] **Description**	教材

一系列零技术门槛的防御建议。

作为基本功和速成训练。并且适合绝大多数政治异议和人权工作者的常规防御工作。

但对于激进派反叛行动来说，仅此是不够的。激进社区请从“ 威胁知识库 ”入手。

本系列内容侧重基础知识，结合 safeguarddefenders 及其他多个类似渠道提供的建议，进行了进一步的本地化和更新（因网络上部分内容已经过时）。

如题所示，本教程的重点是培养学习者在敌对环境中的安全意识 —— 这点事与本站“技术直觉”栏目近似，尽管不完全相同。本教程主要服务于政治敏感人士、记者、活动家、**NGO**组织、人权律师、异议、以及任何想要在互联网上谈论敏感话题而不至于被捕的人。

并不是说这些群体需要 “单独” 的一套安全措施 —— 技术角度的安全性对所有人来说并没有太大区别 —— 而是，上述群体需要一些更有针对性的思考方式。

对于中国大陆的敏感人士来说，您需要考虑的是，当您被拘留、或您的手机电脑被警察没收的情况下，该怎么办。

说到信息安全时，在中国的人们面临的大部分威胁更多是来自人身的，而非来自技术。

其次，相信您在网上或在可能参加过的其他培训中已经接触过大部分安全建议和相关材料，而通常这些材料都汇集了大量的技术性解决方案，其中有很多都是高阶的。

这些培训材料大多缺乏针对如何提升个人安全的具体建议—— 给非专业人士使用的那种通常不是来自高级技术性解决方案的建议（虽然有时候也需要一些技术），非专业人士需要的是那种在操作行为上作出轻微的改变就可以大幅提升安全性的深度讨论。

📌

如果一份安全手册把焦点放在深奥的技术性解决方案上，而没有将它是如何影响我们的日常使用和效率作为考虑， 那它很有可能在一段时间后就被人们抛弃了，只是在初始期会被使用到，渐渐的就会被忽略。

一个真正有用的安全手册应该能在其中找到一个平衡点。

本指南希望以最简单的方式讲述这件事，着重强调可以被纳入习惯操作的一些东西。其中大部分内容我们曾经都提到过，本系列是将它们综合在一起了，但会侧重于中国的一些实际情况。

列表

[image] 来自人身的威胁：如何在敌对环境中保护自己 **S02E01**

[image] 最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己**S02E02**

[image] 手机应该有且只有一个用途：如何在敌对环境中保护自己 **S02E03**

[image] 为最坏的情况做准备，迎接最好的结果如何在敌对环境中保护自己**S02E04**

[image]
[image]

来自人身的威胁：如何在敌对环境中保护自己 S02E01

[image] 关键词	个人 中国 低技术性 威胁模型 数字卫生 自助 自检 预防性
[image] 关联	[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
[image] 创建时间	2025年4月13日
[image] **Description**	教材

在中国，您面临的大部分威胁可能都是来自人身的，而非来自技术……

- Table of Contents

第一部分：了解您的威胁
1、被胁迫
2、疏忽的后门
3、地理位置追踪
4、安全设置
5、破解密码
6、病毒、黑客、**ROOTKITS** 和其他
7、网络连接
8、文件恢复
第二部分：预估您的风险和需求
请仔细回答下面的问题：
1、您需要保护的东西是什么？
2、您使用的哪个设备有风险？
3、您会有什么样的危险？
4、您的威胁来自哪里？
第三部分：基本保护行动

减小可能因为第三方或他人所造成的伤害
电脑痕迹和证据带来的危害
您的数据
手机、电脑和**APP**
您自己
最后
关于密码
指纹、虹膜、面部识别

欢迎来到S02！

[image]

第一部分：了解您的威胁

除非您首先弄清楚自己所面临的威胁，否则有效的防御操作步骤是寥寥无几的。

这一部分将简短的概括在中国的人们可能面临的一些最常见的威胁。

1、被胁迫

在中国的敏感人士面临的人身安全威胁远高于被黑客入侵。关键的威胁就在于被警方或其他人胁迫，让您交出邮箱、云存储或加密数据存储的密码。

2、疏忽的后门

您一定不会花掉一个月的薪水买一扇强大的门，然后忘了买把锁，对吧？或是安装了一个安全的大门和锁，但后门却敞开着？不幸的是，在保护数字安全方面，这就是很多人都在犯的错误。

他们会设置非常高阶的密码，也会清除浏览器的痕迹，但是，却在手机里允许应用程序不需要输入密码就能接入同样的服务，或是用手机浏览器使用同样的服务（比如连接敏感邮箱和账户）。

这就是将后门敞开着，让任何获得您的手机的人或进入手机的任何人都能查看您的一切信息。

最有效的安全意味着您必须分析自己面临的情势，如何完全正确的使用各种服务和功能，然后堵住所有漏洞。

3、地理位置追踪

智能手机比联网电脑更危险。您不会抱着电脑到处走，但是会随身带着手机；于是通过卫星定位、网络连接和手机无线电信号都能轻易的追溯到您的行踪。

如果不设防，任何人都可以轻易的追踪到您，而且很简单，还很便宜。并不需要政府才能实施这些追踪，您的手机从没停止过发送地理位置信号，甚至在没有SIM卡的情况下也是如此。

已安装的应用程序也通常会要求连接地理位置。应尽可能关闭授权。

4、安全设置

大部分的电脑操作系统的自带设置都是以使用方便为主，而不是考虑安全。所以，第一步总是应该查阅所有的设置，做出提升安全性的设置更改。

5、破解密码

暴力破解并不难。使用BF算法（一分钟能尝试千万种可能）可以在一小时内破解出4–6位数的密码。

在设置与您的安全息息相关的服务密码时，比如您的工作邮箱或加密存储，请先考虑一下密码有多容易被破解。一个简短的密码也许能难住街上捡到您的手机的人，但是，在当您成为警方的目标时却没有任何作用。

设置高强度密码、一个长的随机密码，是必须的。

6、病毒、黑客、ROOTKITS 和其他

黑客威胁不是本系列的重点，因为在中国发生的几率不高；而病毒和Rootkits 是比较普遍的威胁。确保您有开启防火墙，有运行可靠的杀毒软件，而且设置了自动更新。

定期更新可以确保您的设备具有识别最新威胁的能力，过期的杀毒软件基本上不能保障您的安全。

7、网络连接

如果当局并不打算拘留您，或是没收您的设备，而是秘密的获取您的信息，您的网络连接自然就会成为攻击的入口。

您是否有定期更换家里路由器的用户名和密码？大多数人恐怕都没有这么做过。路由器的登录密码在网上有公布，几乎所有的路由器都是同样的密码。如果有人能连接您的路由器，那么他们就能进入您的电脑。

8、文件恢复

当您删除一个文件、清空回收站或从电脑转移一个文件到您的USB或其他外部硬盘时，原文件并没有被删除掉，它们全都停留在原来的地方而且可能会停留很多年。

任何有一点点经验的人就能轻易找到它们，通过下载免费的软件，简单的点击一个按钮就能找到任何从您的电脑中 “删除” 的文件。

[image] [image]

第二部分：预估您的风险和需求

即便您的工作没有危险到会被指控和迫害的程度，也基本可以肯定您会遭遇监控 - 大规模监控是统治者的社会控制基石；如果您认识的人被逮捕，您也会面临被传唤 “协助调查” 的状况 —— 您可能会被没收手机和电脑；这种情况下如果您没有提前做好防御准备，会面临很严重的后果。

完善您的日常安全意识可以做到大事化小。

请仔细回答下面的问题：

1、您需要保护的东西是什么？

您工作的相关信息是哪方面的？如果这些信息落到警察手里，将对您造成什么样的影响？更重要的是，会如何影响到与您合作的其他人？

如果您的整个硬盘都被没收了，警察能从中获得关于您和您的工作的哪些信息？又能获得与您联系的其他人的哪些信息，比如资助人、同事、组织成员或队友？

要意识到，如果忽视基本的安全考量会如何影响到您和其他所有人的安全。

2、您使用的哪个设备有风险？

您是否只有一个手机？也许还有另一个卖给同事了？您只用一个电脑吗，还是也会使用办公室的电脑（哪怕仅一次敏感的搜索或下载）？或许您有时候会用朋友的电脑查阅自己的邮件吗？…… 列出一个您在使用的或最近在工作中用过的所有设备的清单。

3、您会有什么样的危险？

如果您是调查记者/公民记录者，一旦情况对您不利，有可能将您定罪的文件资料被他人找到的可能性有多高？如果您是NGO工作者，警方有可能指控您吗，比如针对您的工作内容以及您的资方？或者您是一位当局并不希望被指派法律辩护人的当事人的律师？…… 或者您只是追求自由的公民，帮助传递了被当局封锁的敏感信息？…… 您需要对自己面临的状况有一个清晰的认识。

4、您的威胁来自哪里？

您最担心的是当地的警察吗？还是国家安全局的间谍？找出谁是最可能加害您的人，再来决定适合您的安全方案。

也许您本人并不是目标，但是您参与工作的组织/媒体/社团是当局针对的目标。如果是这样，谁会威胁到你们？尽管您并不是一个重要的目标，但如果有威胁，您的身份会面临什么？

以上这些问题您需要仔细思考并尽可能准确回答，这非常重要。这关系到后面的内容对您本人来说的适用性。本栏目**S01教材的第1～5集及其对应的练习题**与此一致。

[image]

第三部分：基本保护行动

一旦被警察或国安带走，您就几乎失去了所有保护自己的机会。如今

在很多国家都是如此，警察几乎拥有为所欲为的执法权力；他们可以强迫您做任何事，不管是通过威胁您、您的同事或家人，还是通过直接的身体或精神上的酷刑。

在面临这种情况下，唯一保护自己的方法就是在这之前您已经做好了保障自身安全的基本步骤。

这些步骤其实都非常简单，而正是这些看似简单的步骤，对您来说就相当于是否坐牢的终极命运，或是否会导致您最珍惜的人陷入危险困境。

对警方来说,如果要用随机的方法获取关于您的信息，有太多的服务、邮箱、软件，噪音过大很难让他们有效率地获取。所以他们会需要有一个大概的方向—— 关于从何处下手。

如果他们强迫您交出某个服务的登录密码，大部分情况下，他们需要事先知道您最经常使用什么服务。

在中国，他们可能会估计你有微信账户，在越南，他们会估计你有 Facebook 账户 …… 总之，除了这几个特别普遍使用的服务之外，大部分其他的服务他们都需要先知道您在用的是哪一个。

您平时谈论过自己使用的私密服务吗？和谁谈论的？在哪里谈论？…… 想必很多人都谈论过相关内容，大多数人是出于好意，希望将自己发现的“好东西”介绍给朋友，但如果您通过不安全的通讯渠道谈论这些话题、或者说给了不那么可靠的人，而恰好当局正在对您进行“侦查”，他们就会知道该从哪里对您下手了。

本系列将提供大部分普遍问题的解决方案。

[image]

减小可能因为第三方或他人所造成的伤害

首先，您的账户会被当局发现的原因可能来自于您身边其他人的遭遇。

比如，您使用在线通讯与之联络的伙伴、同事、甚至不怎么熟悉的人，他们可能会被警察带走，而他们将你们之间联系的信息交了出去，或是他们有可能出卖了您。

也就是说，对于敏感的工作来往，您需要考虑到的不仅仅是您自己“该说什么”，还有 - 如何存储信息。所以，您首先需要有一个专门的邮件或聊天软件用于最敏感的工作，这个账户或邮箱不应该被用于您的常规工作和私人交流。

这种账号必须使用假名，使用单独的邮箱注册，也不要在任何邮件的内容、聊天会话中包括任何可能显示您的确切身份、地理位置的信息。包括：不要在自然灾害/现象发生的时候通过此分身账户发布 “我这里地震了”/ “我这里下冰雹了” 等等信息，这些信息都很容易识别您的位置，结合其他信息就能识别您的身份。

这样，就算是被第三方查出某个账号与另一个人的来往记录，他们也不知道那是谁；就算被捕的人供述出了这个账号属于您，您也有一些程度的否定空间。

这就是为什么我们建议您分身，并采取假名身份从事敏感的交流和工作。

[image]

安全问题的最大的顾虑之一、也是您自身最难以控制的部分在于，它会取决于与您合作的其他人的安全意识。所以，您需要尽可能地与具备足够安全意识的人合作，并为安全意识足够但是合作面不同的合作者分配不同的知情等级。

您最好能在最敏感的互动中使用带有自动销毁（阅后即焚）功能的聊

天软件，比如说一小时或一天后即自动删除。比如 Signal、Session、wire、tox 等等，销毁的消息永远无法复原。

[image]

返回：[image]一系列安全的即时通信软件和服务

notes：在本站“工具”专题中搜索“IM”以找到更多选项。

自动销毁功能非常重要，尤其是当您与一个不完全信任的人通讯时，或与某个非常缺乏IT 操作技巧的人联系时。用起来也很简便。

[image] 在咱这儿，交朋友不看颜值

电脑痕迹和证据带来的危害

一旦您被带走，或是您的电子设备被查抄，当局很可能启动技术化的取证分析；再通过他们所掌握到的各种开源情报和人力情报，更容易强迫您交出某些账户的密码。一旦他们成功，他们所找到的这些信息就很有可能用于对您或您的合作者不利。

比如浏览器，通常可以存储大量的数据。最明显的类型是一个链接到邮箱服务的书签， 或已访问的网站 cookies 和更进阶的数据，还有登录信息甚至是密码。

您可以将浏览器设置为自动删除此类信息，但是这意味着每次当你打开浏览器时，都需要重新登录每一个网站，包括社交媒体，购物网站等。加上您也没有使用书签功能，这就会让整个使用电脑的过程非常低效，而且看起来也很可疑。

[image]

相反，您应该做的第一件事情是使用双重浏览器策略。一个浏览器用于平日普通的浏览和使用，另一个浏览器用于最敏感的邮件收发和相对敏感的资料搜集工作。

用于工作的浏览器应该设置为关闭时自动清除所有痕迹，也需要添加特定的安全插件，以便协助浏览器的清除工作，更彻底的移除掉更多的痕迹。当然，Tor是最好的，可惜那些寡头企业的服务会将Tor用户视为可疑（《二等公民》），权利组织正在就这个问题进行交涉。

此外，与浏览器一样，操作系统也总是在收集您使用电脑的一切数字痕迹。这包括网站访问、Word文档的打开和编辑、临时数据和文档的复制等等几乎所有动作。对于拥有大量资源的警方和政府来说，获取这些信息并不难。

[image]

返回 - 相关内容汇总：[image]数字取证

要应对这个问题，您需要用到一个专门清除这些痕迹和电脑内临时数据的软件，幸运的是，它用起来也并不难。

您的数据

当然最关键的问题就是您的所有文件了，不管是存储在USB、手机、外部硬盘或电脑内的文档、视频，或照片，保护这些信息的唯一路径就是将它们存储在一个具有较高安全系数的地方，比如在电脑内的一个加密的、非常隐蔽的硬盘内。

也就是说，如果只是基础加密，警方可以通过直接或数据分析的方式就能找出。所以，要真正的保护好您的信息，就需要使用到“隐藏的”加密空间，让他们根本不知道您有加密的信息存在，这样他们也就无法通过威胁或酷刑让您交出密码。

而且，这个步骤的操作比听起来简单多了。

您也应该将数据存储简单化—— 不要将所有的工作文档都存进这个空间，而是仅存储那些有必要的。

大概浏览一下您的旧文件，很有可能大部分文件您已经不再需要了，草稿、已使用过的文件、协助文件等等，这些都应该彻底删除。仅存储那些真正有需要的文件。

您也可以将需要保留但可能不会经常用到的旧文件转移到安全的云存储上。您需要使用一个安全度高的、在中国没有服务器的云存储服务。最好是自己的云。

另外您也需要留意浏览器中的信息，要确保警方无法发现您所使用的云存储是什么（如果您搜索过它的名字，那就不好了），也无法获取登录方式。

手机、电脑和APP

在工作中要将电脑和手机的使用分开，这两者之间不要有重叠。您之前所做的安全步骤都有可能因为疏忽的使用手机而毁于一旦。

自动销毁脚本文件、保持清除浏览器痕迹的动作都很好，但是，如果警方都能在您的手机上轻易的找到这些信息的话，那还能有什么用？

人们习惯于通过手机内的App进入账号和服务。使用手机App不仅相当于给予警方直接的（虽然有限的）进入您的账户的通道。比如邮箱，就算是您为手机的App额外设置了密码保护，但这样还是暴露了您在使用的服务是什么，警方还是可以强迫您交出密码。

手机可以让您所做的电脑安全设置功亏一篑，这样的不幸发生过很多次。

请务必仔细研究手机的使用方式，避免在手机中使用敏感工作相关的、或可能被察觉到您在使用的服务应用程序。

此外，不要用手机内的浏览器进入敏感工作邮箱，因为手机内的痕迹

是几乎不可能清除掉的。而且，在手机内彻底的删除也非常难。

坚决不要用手机存储任何敏感的文件信息，包括不要临时下载任何工作文件后再转移到电脑。

您自己

最后，您本人的操作安全性水平，对您自己和周边人都至关重要。

要保护好您自己的信息、文件和数据，就需要做好充分的计划。

除了做出必要的风险评估之外，您也需要做好预备计划 —— 比如在被带走的情况下您会做出哪些反应？而且还要将您的计划告知几个最信任的、而且是那种不太可能会被带走的朋友。

一旦被审问，什么样的信息是你该说的，什么样的信息是你一定要保护的？ —— 因为一旦进去，您总是要说出一些东西，否则很明显他们会知道你在隐瞒。您需要迅速衡量不同信息的危险程度，并尽可能准确地抓住要点。

同样地，如果您有同道， 你们需要一起讨论出一个每个人都同意并坚持遵守的应对方案。您也需要考虑到他人最有可能会放弃保护的信息是什么。

在政治领域有一句俗语：绝不要撒那种公众能够发现的谎。对您来说则是：不要撒警方能够发现的谎。关于这点并没有技术性的解决方案，只能靠您自己的谨慎和智慧了。

最后

在像泰国、越南、中国等很多国家，获取未实名认证的SIM电话卡可以说是很难的。 这也就意味着当所有的互联网服务供应商（ISP）要求您实名设置网络连接时，也就产生了问题。

警方可以任意要求任何通信公司和网络公司的日志记录。这些公司通常都有将客户使用服务的记录存储起来，比如他们会记录下您使用手机的情况，包括您的地理位置、网络使用情况等等。

也就是说因为上述，您在手机内所做的一切为了保护数据、隐藏使用的服务等步骤都可能变得徒劳。幸运的是，您可以通过使用**VPN**或**TOR**，对互联网服务供应商隐藏上面提到的大部分信息。

[image]

返回：[image]使用Tor保护自己时千万不要做这9件事

返回：[image]如何检查您的VPN连接是否实际加密

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

手机的安全问题不那么容易解决，所以对于敏感工作来说，还是建议您使用电脑，而不是手机。

关于密码

用强密码就不用说了。密码管理器可以帮助您创造超强的密码，并且您只需要记住一个主密码即可。

但是，如果警察破门而入抢走您的电脑，而您的密码管理器就在电脑上 …… 您知道那将有多糟糕。

所以，密码管理器最好是放在一个隐秘的加密的USB中。必须能尽可

能确保不被找出来。

所以，最好的依旧是上述思考方式：让对手找到错误的东西，一旦找到，他们就不会意识到还有其他东西存在。于是您可以使用两个密码管理器，其中一个就放在电脑上，用主密码锁住，在被威胁得足够程度的情况下交出那个主密码，而这个管理器上存有的只是一些无关紧要的密码，而真正重要的东西在另外的隐藏的地方（您自己知道）。

所以这还是需要强调分身：如果警察知道您在推特活跃，而您交出的密码管理器上没有推特密码，只有微信密码，这就很可疑了。于是您的两个密码管理器恰恰应该是切分不同身份的存在，让搜查者找到那个无关紧要的身份，他们就很可能不会想到您还有其他身份。

[image]

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

指纹、虹膜、面部识别

尽可能不要使用这些东西。它们看起来很高大上，但这些东西更危险—— 如果您的密码被泄露您能轻易的再建一个新的，但您却不能重建一个新的眼睛和指纹。

并且，审讯者只需要抓住您的手，或固定您的脑袋、扒开眼睛，就可以强制解锁，您是不是处在清醒状态都不重要。所以，不要使用生物识别解锁方式会比较好。

[image]
[image]

最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己S02E02

[image] 关键词	个人 加密 操作安全性 网络
[image] 关联	[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
[image] 创建时间	2025年4月14日
[image] **Description**	教材

操作安全性比技术本身更重要。

- Table of Contents

原则
1、极简主义
2、零收件箱策略
3、无回复约定
4、紧急计划
关于浏览器
1、双浏览器策略
2、将文件保存到正确的位置
3、网络连接
3.1 HTTP VS HTTPS
3.2 路由器
3.3 ISP、**IP**地址和**MAC**地址
4、**Firefox** 浏览器和扩展程序
A、**BetterPrivacy**
B、**HTTPS Everywhere**

C、KeyScrambler
高级加密（技术性解决方案）

[image]

期待每时每刻全面抵制所有威胁可能不太实际。于是建议您现实一些，把焦点放在主要的威胁上。

要了解到对您不利的各种威胁和相关技术是一条漫长的路，这也是为什么建模并分析并理解您所面临的实际情况很重要。

[image]

返回练习：[image]S01E05-T3 确认可能遭受的所有威胁

坐下来仔细分析下您自己的情况，确定个人倾注的焦点是什么，了解您面临威胁的前因后果，它们来自哪里，如何让它们远离或是变得没有那么严重，这些都很重要。

以下是一些技巧，准确说应该是原则，一些非常简单的习惯就能帮助您在很大程度上应对常见威胁。

原则

1、极简主义

即使是专家也会觉得管理多个程序的安全维护要比少数几个程序的安全维护要困难得多。多一个程序就多一份威胁。这就是为什么我们说极简主义是一种生存智慧。

[image]

返回：[image]少即是多：变得难以被追踪的简单方法 S03E05

您要做的第一件事就是查看电脑和手机里的所有程序，看是否都是经常使用的？如果没有经常使用，删除它们。仔细考虑它们是否是必要的？如果不是，删除他们。

如今一部手机能很快被各种聊天软件填满，但是不一定都是真正有必要使用的，如果多半时间用不到的话，那就删除它们。这也是一个为手机和电脑腾出空间和加快速度的加分项。

中国的应用程序往往没有强大的加密功能。中国程序收集到的用户信息不受法庭保护，而是随时可以教给政府和警方在他们需要的任何情况下浏览。

因为对加密的缺失，数据也很容易被任何人获取。

[image]

延伸：https://iyouport.substack.com/p/--041?utm_source=publication-search

就如硅谷巨头的服务为美国间谍机构构建“后门”，能给政府监视者一个直接的通道连接到公民的电脑和手机，甚至是在您不知情的情况下。中国的技术寡头当然也会这样做。只要一个程序，比如微信，就能造成您整个手机和电脑的安全威胁，所以，您必须非常小心。

[image]

返回：威胁矩阵 👁🗨大规模数字监控

[image]

延伸：

[image]

2、零收件箱策略

邮箱面对的最大威胁可能不是被高级黑客入侵，而是当您被捕时，警方强迫您交出您的邮箱密码。

如果被拘留，警方就有机会获取您的邮箱登录密码。就算您本人坚持不交出密码，您的同事、朋友、队友、合作者、熟人等等都有可能交出他们的密码给警方，这样您和他们之间的所有通讯记录都会被警方看到。

这就是为什么零收件箱策略能带来便利，是为您带来安全的重要原则之一。

设想在您被带走后您交出了邮箱密码，零收件箱策略就能保证里面没有任何内容可以被人看到，简单来说就是保持您的收件箱（包括其他的文件夹）为空。

更重要的是，让您的队友、同事、朋友们也必须如此操作。您非常有必要与注重安全的人交往。如果您推测对方可能不怎么擅长安全操作，那就不要通过任何互联网媒介与对方讨论重要信息。有话当面说。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

3、无回复约定

无回复约定是零收件箱策略的延伸版。如果您的邮箱确实被警察或黑客登录了，他们只需要稍微等一等就能了解您的大量信息。

这是因为在通信时，我们大多数人通常都是在当前的邮件下点击“回复”，而不是重新写一封。鉴于此，早前的通信内容会自动包含在同一封邮件内，通常这样来来回回的回复可以持续很长一段时间；其结果就是，一个简短的新邮件会包含一大段更长的早期邮件内容。这非常危险。

如果您的邮箱被控制了，控制的人只要等待有人用回复功能回复你的邮件，就能读到你们先前的所有通信内容。

所以，当您用邮件回复您的队友时，请避免使用邮箱的回复功能，如果必须用的话，确保删除原先的邮件文字。这样做能在被拘留的情况下，即便警方获取了密码并蹲守，也只能获取到较少的信息，让他们难以挖到能针对您的东西。

再一次，请告知您最经常通信的朋友或队友也要这样做。

没有任何人能独自实现安全。我们必需共同遵守一套安全文化，实现彼此保护。

[image]

4、紧急计划

在您的同事或朋友被警方带走时、他们的电脑已经被警方没收的情况下，一切都已经太迟了。如果您等到那时候才与同事或朋友讨论如何删除敏感材料，警察会给您扣上一个尝试销毁证据的罪名。

您必须在这些情形发生之前先准备好，必须知道在事情发生之前、 之中、之后分别要怎么做。当然，也必须知道您的朋友和同事会怎么做。

您需要有一个计划。唯 一的方式就是提前与重要的伙伴讨论、协商好如果我们中有人被带走、或电脑被没收的情形下，您或其他人应该如何应对。是否所有人都将手机恢复出厂设置呢？还是再三确定收件箱是否为空？还是你们所有人都重设密码，将电脑格式化？……

[image]

返回：威胁矩阵和自卫措施 [image]数字取证

不管你们怎么决定，最重要的是所有人都做同样的操作，并且彼此间要知道对方会怎么做，且相信彼此都能做到。

这被称为制定并遵循 “安全协定”。如果您自己做了很多事并且处于安全状态，但是你们中有一个队友没有这样做，这就会让您的尝试和努力变得毫无意义，并且也会为其他人带来风险。

和您的队友坐下来谈论这件事，记住，如果您的工作网络包括多个团体或同事，或针对不同问题的人权工作者，他们不 一定都知道对方是什么样的人，有的人比其他人做的事更加敏感，您可以和不同的团体建立不同的紧急计划， 这一点非常重要 —— 建立一个紧急计划就是建立“安全协定”。这样每一个人都知道该怎么做，而且也很容易遵循。

如您所见，这些安全措施都涉及到团队合作，也是我们一直强调的 —— 安全不是您一个人的工作；任何与您交往的人都有可能出卖您。所以，您不仅需要和同等安全意识的人合作，同时也要注重团队培训和协作技巧。具体做法参见本站专题栏目。

[image]

返回：🔥反渗透/线人&减轻背叛的损失-AntiInfiltration&informant

接下来我们将谈论浏览器的问题。正如此前强调过的，手机本身是不安全的东西，让手机获得足够多的安全相对较难，于是对于不够熟悉技术的行动者来说，非常建议您使用电脑或笔记本进行敏感操作，而非手机。

[image]

关于浏览器

当使用浏览器的时候，有两件事会发生：

1. 是您访问的网页会收集您的信息；

1. 同时电脑也会收集您使用浏览器的记录，这些信息包括Cookies、LSO虚拟数据、键入的密码、浏览器的历史记录等等。

您可以在下面看到详细介绍，这些是威胁面，了解它们很重要。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

便于运行正常，大部分的网页都用一种 JavaScript 编程，这样浏览器和电脑都很容易获取网页Bug和病毒，再通过浏览器感染整个电脑，这两个方面都需要注意。

幸运的是有办法解决这个问题，而且第一步只需要改变操作习惯就可以。

[image]

返回：[image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

1、双浏览器策略

在极简主义的原则下可能会建议您只使用一个浏览器，并设置为在关闭时自动删除所有数据。但是这取决于您用于个人目的的浏览器使用需求量，如果在使用每个服务时都需要重新登录一次密码，操作起来会很没效率，也非常不方便。所以推荐您使用双重浏览器策略。

也就是分身 —— 切分您的日常操作和敏感重要操作。

选一个浏览器用于私人上网，再选一个用于敏感的工作。敏感工作的

浏览器可以使用 Firefox，它并不是最快的浏览器，但是允许重要的安全附加组件和扩展的设置。

不敏感的日常操作可以使用 Chrome。

双重浏览器意味着用于日常上网的浏览器您可以维持以前的上网习惯，也不用被附加组件和扩展耽搁太多时间，但是，敏感操作相关的上网习惯虽然麻烦但肯定能明显的提升您的安全性。您值得培养这一习惯。

一旦做好决定，就要持续下去。

接下来的技术性解决方案针对 Firefox，关于如何更安全的使用 Firefox。

2、将文件保存到正确的位置

系统浏览器默认的下载和存储文件夹是安全的一大威胁，却少有人注意到这点。

如果没有做任何设置，您从浏览器下载的文件都会被存储在操作系统的硬盘内，要彻底删除信息是件困难的事；所以，重要的是，在使用浏览器和下载时，使用能够自己控制新文件将被存储的位置的方法。

最好的方式是在您的加密硬盘内新建一个文件夹。不过要知道，如果您将文件存储路径设置到了您的加密硬盘，要是在您的加密硬盘没有解密的情况下下载某个文件时，文件会在不通知你的情况下直接被存储到最初默认的路径位置。

关于下载的位置要记住两件事：1、总是存到同一个位置；2、要储存到您的加密硬盘。

不要随意将新的文件保存到桌面。

[image]

3、网络连接

3.1 HTTP VS HTTPS

现在有很多服务都提供登录加密，但就算有这个功能也不完全可靠，因为那些公司会记录下您的信息，并在政府需要的时候交出去。

如果要知道您登录的网站是否有提供加密功能，很简单就能辨别。只需要看下浏览器的地址栏就知道。未被加密的连接在网页的开头显示 HTTP (http://www…)，有加密的连接显示 HTTPS (https://www…)。通过 Firefox 中的 httpsEverywhere 浏览器就会自动使用 https 加密。

3.2 路由器

现在大部分上网方式都是无线连接，无论是在家里、办公室还是在咖啡店。于是您需要了解一些无线路由器的基本运行原理。

进入路由器需要用户名和密码。它们通常都被贴在路由器的背面或底部。所有的路由器几乎都是同样的，通常用户名为 “admin”，密码为 “password”。就算有些可能不一样，但是同一个品牌和型号的路由器都会用一样的用户名和密码，所以还是很容易找到的。

也就是说，利用这个信息，任何人都可以进入您的路由器。如果他们能进入您的路由器，也就相当于控制了您的网络， 他们可以轻易的安装程序监控你的上网日志，甚至拦截你的网络。

大部分人几乎从来不会对路由器的用户名和密码进行更改。可以通过浏览器键入路由器的IP地址（通常是192.168.0.1）进入路由器，这个

IP地址也会被写在路由器盒上。通过登录路由器，您可以进行更改用户名和密码的操作。

一般来说 192.168.0.1，192.168.1.1，10.0.0.1 是最常见的IP地址可登录到路由器的管理面板。如果它们中的任何一个都不起作用，可以通过这里的指南查找设备的默认路由器IP地址。

另一个需要注意的关键是，当使用无线网络时，无线网络信号需要被加密过，否则上网时传输的所有信息都可以被周围的人读取。

如果没有进行加密，任何人都可以连接并使用您的无限网络信号， 并看到这个连接下的所有上网记录。您的无线网络信号的名字就是那个您通常连接上网的名字 （叫SSID），如果连接时要求输入密码，则表示这个信号是有加密的，如果没有密码，则表示没有加密。

一旦进入路由器后，您可以更改SSID名称，也可以选择加密网络信号。用于 Wi-Fi 路由器的标准加密通常被叫做 WPA2（WPA3）。要启动加密，您需要设置一个密码。

因此既有用户名和密码进入路由器，也有账号登入您使用的无线网络信号。它们之间并不一样。 如果您想弄清楚具体如何在路由器中做这些更改，在搜索引擎上键入您的路由器名字和型号就会有很多步骤图能帮到您。实际比看起来要简单很多。

3.3 ISP、IP地址和MAC地址

在一些国家，一般来说使用的网络都来自国有的几个网络服务供应商（ISP）之一，您甚至在很大程度上都无法选择。这实际上带来了巨大的风险，因为在设备上所做的很多步骤都可能会因此而变得徒劳，因为向您提供网络服务的ISP也将自动记录下您在这个连接下所做的一切动作。

不同的供应商将这些信息存储的时间长短不 一，但都会储存。

当连接上网时，您家里的路由器会通过网络服务供应商（ISP）将您与更广大的网络相连接。也就是说，您家里的路由器连网时首先都要先通过ISP服务。审查也就是从这里开始的。

而您上网的足迹，无论是由ISP所掌控的您的连接，还是您访问的网站或您的电脑手机连接的服务，都是通过您的IP地址和MAC地址来追踪的。

IP地址就是您的上网连接地址，通常很容易被辨认和追踪。如果通过无线连接上网，您的IP会改变 (为动态)，但是您的ISP总会知道所使用的网路连接是与哪一个IP地址相联的。

您的电子设备也会有一个MAC地址，每一个有联网的设备都会有一个MAC地址，这个独特的MAC 地址是专门为实质的硬件生成的。一旦硬件被产出，MAC地址就会随机产生。在通常上网时MAC地址倒是不会被分享出去，但IP地址是可能对您造成问题的。

幸运的是一些非常简单的方法就可以避免被ISP监视您的上网活动，或被网站追踪您的IP地址，比如使用 VPN 和 TOR。

简单来说，VPN和TOR 都可以避开ISP的监视，大部分情况下也能加密您的上网行踪，对您的安全和隐私来说是必不可少的。

[image]

4、Firefox 浏览器和扩展程序

打开火狐浏览器，点击右上角的设置就能找到附加组件的区域 ，在扩展标签下能显示所有已安装的附加组件。

A、BetterPrivacy

通过安装这个附加组件有关闭浏览器时自动删除数据功能的选项。安装了这个组件您才能彻底的删除 LSOs —— 一种难以清除的新型

Cookie，也叫 Flash Cookie。

安装后，点击选项，选择选项&帮助列表，点选当 Firefox 退出时删除 Flash cookies，点选同时删除 Flashplayer 默认 Cookie，以及点选删除 Cookie 时同时删除空的 Cookie 文件夹。

B、HTTPS Everywhere

如上所述，这个附加组件能自动开启支持HTTPS加密。下载后能在 Firefox 的工具栏看到它的图标，点击启用就能自动运行此功能了。

C、KeyScrambler

与上面的附加组件不一样的是，这个组件不能在附加组件区域安装，而需要下载，先搜索 KeyScrambler，选择下载并像普通程序一样安装，电脑就能在重启之后运行这个程序了。

高阶的黑客能通过在您的电脑安装一个键盘记录程序，获取您键入的所有记录，包括用户名和密码。通过对登录用户名和密码按键的自动加密，这个小程序可以帮您抵御此类攻击。

现在您已经完成了敏感操作所使用的浏览器保障的一半，接下来还需要在设置区域做一些简单的更改。

只需要注意几点即可：

1、点选总是“询问保存文件的位置”；

2、搜索建议设置为默认duckduckgo；

3、允许在隐私浏览窗口中使用跟踪保护，在历史纪录下，点选不记录历史，在 “地址栏” 的选项中确保每一项都没有被选中；

4、在 “安全” 标签下，勾选常规下的所有选项，在 “登录信息” 那里不要选择 “主密码”，在这个页面也顺势点进已保存的登录信息内看是否有任何登录信息被保存了，如果有的话，请删掉。

5、不要使用同步功能，也不要将Firefox与其他的邮箱账户等绑定，不要用邮箱登入Firefox浏览器；

6、在 “更新” 栏下点选自动安装更新，并确保有点选自动更新搜索引擎。

高级加密（技术性解决方案）

创建一个隐藏的加密空间，需要使用 Veracrypt 或 TrueCrypt，将其下载到电脑或USB都可。**USB**会更加安全，不过需要先将USB插入电脑才能操作。

同样，总是要记得将文件直接下载到您将要安装的位置，不要下载到桌面或默认的下载位置。

与基础加密不同，当要使用隐藏加密空间时，就好比下载一个新的文件一样，需要打开 Veracypt 并加载隐藏加密硬盘，就会跳出一个看起来和普通的硬盘或USB一样的窗口，一旦使用结束后点击退出即可。

新建的加密空间叫加密卷。您一定听说过，而且网上有非常多的教程，这里就不做具体介绍了。简单说说您为什么值得这样做 —— 在敌对环境中。

防止他人进入到真正的隐藏加密空间 (内部加密卷) 的能力被称为 “合理推诿”，意思是通过交出外部加密卷密码让事情合理化 —— 让对手以为他们已经拿到了“隐藏的秘密信息”，而实际上您并没有交出内部加密卷中真正敏感的材料，这是保障自身安全的一个关键。

请注意，要想让它真正起作用，外部加密卷就必须看起来是 “可信的”。

在这里 “可信” 的意思是：在外部加密卷 (诱饵) 内的信息必须是很明显你不会愿意分享出去的。一旦您被强迫交出加密空间密码（外部加密卷），当警方读取里面的资料时，要令他们相信那是你正在努力保护的东西。如果里面的内容为空，或只是电影音乐文件等， 警察就肯定不会上当，会继续向你施压。

所以，确保在外部加密卷内存入的是很明显的敏感文件 —— 但不是会让你坐牢的那种东西。比如，您可以存一些银行账户相关文件、一些禁书的PDF文档、同时也应该放一些工作文件，比如您写的报告之类的东西， 但是必须让警方用不到的那种。

请记得每过一段时间添加一些新的文件到外部加密卷，让它看起来像是您一直在使用它。如果有更高的安全系数要求，可以多复制几个文件到外部加密卷。

总之，不要将真正的敏感文档存在那儿，这里只是作为诱饵。设立诱饵的原因是让警方远离您真正的敏感资料，一旦他们以为已经找到了所有的信息，并满意了，那他们很可能就不会继续施压了。

需要不断更新外部加密卷的原因是，每个文件和文件夹都有显示这些文件最后被转移或修改的时间的数据，如果警察进入您的外部加密卷发现在过去两年内这些文档都没有被动过，那他们会意识到你并没有在使用这个硬盘，要么是一个老硬盘或圈套，这样也会再次向你施压以获取更多的信息。

要建立这一套系统最简便的方式就是先将所有的工作文件移到您的内部加密卷；浏览一遍所有文件的内容后，将一些工作相关但又不是特别敏感的、不包括人名、细节、或可能牵连他人的信息文件，存到外部加密卷。

鉴于外部加密卷应该是可信的，建议您存入类似下面这些东西：

- 密码清单，比如网上购物网站的登录密码、私人的社交媒体等等，与工作无关的个人隐私；
- 也许在过去您写过一些肉麻的情书或个人笔记，如果有，存进来；
- 也许您有与情人发过一些私密的通信、照片，存进来……

总的来说就是，外部加密卷以普通角度来说会非常安全，只有在被警方强迫打开的情况下才有威胁。 如果事态很严峻，到了他们要强迫您交出了密码的时候，就要保证您在里面存入了这些个人的信息以供警察读取。

请注意，要让事情看起来可信，就不要一开始就轻易的交出外部加密卷的密码。如果被问起您还是要先拒绝，作出一副无奈的样子，推脱多次、挨一些打，再很不情愿的将外部加密卷密码交出去，否则对手可能会起疑。

如果他们相信了，真正敏感的信息就会保持安全。当然，没有人愿意让警方看到您发给情人的裸照之类的东西，但是与坐牢比较，您明白该怎么选择。

如果您没有上面提到的这些个人隐私类型的信息，建议现在建立几个存进去，如果有必要的话也可以PS一个。这真的意味着自由与坐牢的区别。

请注意，本系列教材提供的都是根据最常见的胁迫您可以采取的应对方法以及相关工具，您当然可以在此基础上更为深入地开发出创意性的方法 —— 那些我们不能说的东西（一旦公开说出，它们可能就失效了）。创造力是几乎每一种成功的关键，这需要您来完成。

[image]
[image]

手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

[image] 关键词	移动设备 自助 自检 防御
[image] 关联	[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
[image] 创建时间	2025年4月15日
[image] Description	教材

操作习惯比软件更重要！

- Table of Contents
自动登录与交叉服务登录的危险
尽可能不使用云
向正处于安全威胁的人发送信息
发送可以自动销毁的邮件
在真正有必要的时候才添加附件
要彻底删除
关于手机安全
“我的手机被窃听了吗”
如果您使用手机，请注意
中断通讯
自动同步和云存储
关于地理位置追踪的提醒
如果 …… 怎么办

[image]

Edward Snowden: "Both Apple and Android devices unfortunately

are not especially good in protecting your privacy."Every phone, even when the screen is off you think it's doing nothing, but it's screaming 'Here I am'.""They can see everything about you. They can see everything about what your device is doing, and they can do whatever they want with your device.”
attachment:8fd091a8-c6a3-42da-b26c-085a1be503d7:cXRgqikhBzdSUR_F.mp4

自动登录与交叉服务登录的危险

自动登录有很大的安全隐患，特别是当进入了一个账户就能进入同一个服务商的其他账户的情况。 比如在浏览器登录了 Gmail 后，不用重新登录就能进入到 google drive 和 Youtube 等等。

同样的情况也适用于其他家族式服务商，比如苹果、微软等等。

📌

延伸：https://iyouport.substack.com/p/42b?utm_source=publication-search

避免这类情况的最好方式就是尽量一家公司只使用一个服务。假设您在用 Gmail，那云存储的服务就不要用 Google Drive，这样能避免自动登录和账户同步的威胁。

此外，绝不要启用任何邮箱或云服务的自动登录和同步服务。

现在的很多服务都擅于用同步（Auto-sync），比如您在手机中使用了 Chorme，再在电脑的 Chrome 浏览器中登录，如果没有禁用同步功能， Google 就会将这两个不同设备中的浏览器信息同步合并。在电脑中保存的书签都会出现在您的手机中，浏览器历史记录、保存的密码等等都会被同步。这是一个很大的问题，您的敏感工作浏览器不该有同步。

尽可能不使用云

云存储通常是指信息的线上存储。有些云服务只用于工作文档的备份，有些用于更新和存储电脑内的设置和程序，还有些如协作平台在运行，可以用来与他人分享文档以及同时编辑等。

请注意，一般来说线上存储都不安全。鉴于这个原因，敏感工作文件绝不要使用 OneDrive (Windows), iCloud (Mac)和 Google Drive 服务。

最好的是，构建自己的云。网上有很多教程。

延伸：https://iyouport.substack.com/p/nextcloud-?utm_source=publication-search

您可能不知道自己已经有了云服务。比如，如果您有 Gmail 那就肯定有 Google Drive， 如果在用 Mac 电脑，那就是有 iCloud，如果是在用 Windows系统或是用 Hotmail，那一定有 OneDrive，很多的这些云服务都是随着手机和电脑进行预先安装的。

首先，全面检查您的手机和电脑，看有哪些服务和App被安装和启用了，没有使用的都应该设置禁用。特别是现在的手机都是自带保存照片、视频和文档等个人信息的配置，这些都可能会成为威胁，特别是在手机里的这些程序几乎都是不需要输入用户名和密码就能进入的。

移除和卸载那些您不会使用到的云服务。

其次，不要依赖于用手机里的App进入云存储。App确实很方便，但很容易带来风险。任何拿到您的手机或电脑的人都能轻易发现您在使用什么服务，然后强迫您交出用户名和密码。

记得要用工作浏览器通过VPN登录到云服务（见上一集中的内容）。

不论如何，至少不要使用中国公司提供的云服务。

[image]

向正处于安全威胁的人发送信息

如果您需要向某个可能正处于安全威胁的人发送信息，不管是问问题、普通聊天还是给予指示，都应该以尽量减小潜在风险的方式。

这个人可能正面临被拘留或绑架（强迫失踪）的风险，也可能已经成为网络攻击的目标，或者仅仅在于您无法信任此人能安全的保障您所发送的信息 ——你们之间没有安全文化共识。毕竟不是所有的人都会遵循安全操作，这样一来您自己是否能够以最小化潜在风险的方式发送信息就显得尤其重要了。

您应该尽可能发送内嵌的消息：就是内容在邮件的正文内而不是用一个附件的形式。如果不是特别的有必要都不要使用附件。如果非得用附件，则尽量减少附件里的内容，在添加附件前将文档内的元数据清除掉。

发送可以自动销毁的邮件

ProtonMail 因为自动销毁功能受到好评。类似的服务如 Signal 等等，也是推荐的。您可以在给某人写一封邮件时设置一个时间，这个时间从您发出这封邮件时就开始计时，这一点很重要，时间是由您发出邮件时开始计时，而不是从读取时开始计时。

您可以设置一个合适的时间，比如一 小时或一天等，这个时间点一到，邮件就会被自动销毁，而且是在您与收件人双方同时销毁。确保当您发送了这样一个安全邮件时，收件人能及时的读取邮件。

另外一个优点在于，就算您的收件人使用的不是 ProtonMail，也仍能发送高度安全的自动销毁功能邮件。

收件人会收到一封邮件告知如何取得这个 ProtonMail 的邮件内容。一旦这个预设的自动销毁时间已过，这个读取 ProtonMail 的链接即失效，也就是这些信息已经被自动销毁了。

在邮件中的附件也会被销毁，不过，如果之前已经从链接中下载了的文件就不会被自动删除，所以，尽可能的不要添加附件发送。

使用自动销毁的功能意味着您不需要担心收件人是否有严格遵循安全使用电脑的步骤，比如删除邮件的习惯，或是坚持零收件箱策略等（如前文所述），因为您知道在这个设置的时效一过，不管收件人的行为如何，这个邮件就会被自动删除。

如果您刚发出邮件，对方收件人就被警察带走了，您发送的信息也仍然会在时效内被自动删除，当然还是希望在被邪恶的第三方看到之前。

[image]

在真正有必要的时候才添加附件

任何文档中都包含比您想象的要多的信息。不止是文档中的内容，还有元数据。

元数据所包含的信息是一旦您建立了一个文档，建立文档的这部手机或电脑的型号、用户名、地理位置，甚至手机自动面部识别功能所标注的名字等等。

如果您确实需要建立一个文件作为附件发送，要考虑到下面几个点：

- 不要包含照片、Excel、图表等信息，在保存文档前检查和删除

所有元数据；

- 不要发送 Word、excel 等形式的附件，将文档转换成PDF再发送；

- 为 PDF 文件设置密码保护。

当您将 word 或 excel 文件转换成PDF格式时，会有为文件设置密码的选项，建议您将这个选项作为必要的操作，然后使用安全的聊天软件，如 Signal、wire 等，告知您的收件人打开文件的密码。

返回：https://iyouport.substack.com/p/macpdf?utm_source=publication-search

返回：https://iyouport.substack.com/p/zippdf?utm_source=publication-search

有密码保护的文件就像被清空的收件箱，能保障收件人避免受到具有伤害性的攻击，毕竟他人想要获取它有一定的限制。大部分您收到的附件一般也不需要一直保留，一旦用完附件中的信息，比如更新一个档案、添加到一篇文章、完成一份上诉状等等，就应该安全地将这个附件档案删掉。

最后，记得总是遵循 “零收件箱策略”，也将这个习惯普及给其他与您频繁联系并可能面临风险的朋友。“零收件箱策略” 是保障您的人身安全的重要武器。

返回：https://iyouport.substack.com/p/-microsoft-office-

[image]

要彻底删除

良好的IT使用习惯、强大的密码和加密空间都是非常好的保护，但是，如果您无法安全地删除文件，以上这些都将无效。

当您点击删除文件、或清空回收站时，实际上信息都没有彻底被删除，您以为昨天或是两年以前已经被删掉的文件，也仍然躺在那儿随时等着被任何心怀不轨的人翻出来。

对那些有必要保护信息和资料的人，必须说如何彻底删除是一个最大的问题。被删除的文件也许无法在搜索栏中被找到，但其实它们仍然躺在那儿，很轻易就能被警察或间谍找到，操作方法并不难。

[image]

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

删除的概念对于很多人来说还是一个知识盲点。就算对信息安全有一定认识的人，也常常忽视了安全删除的问题。

延伸：https://matters.news/@iyouport/27467-%E6%B8%85%E7%A9%BA%E5%BA%9F%E7%BA%B8%E7%AF%93%E6%97%A0%E6%B3%95%E7%9C%9F%E6%AD%A3-%E5%88%A0%E9%99%A4-%E6%96%87%E4%BB%B6-%E5%A6%82%E4%BD%95%E5%BD%BB%E5%BA%95%E5%88%A0%E9%99%A4%E4%BB%A5%E6%8A%B5%E5%88%B6%E4%BB%BB%E4%BD%95%E5%8F%96%E8%AF%81%E5%B7%A5%E5%85%B7-bafyreidly5o2a7rmzprp3ahx4ydaottywsgjpfkwf54wfewvjwywgpojze

除上面文章中介绍的方法之外，还有一种更简单的方法。

CCleaner 是一个能帮助解决很多问题的程序。它不仅能确保删除电脑所收集的各种信息，比如您操作的痕迹、cookies、临时文件、在编辑的word文档数据等等，而且还能确保擦除电脑的空闲空间和 “已删除” 的文件。

注意：如果您用的是SSD固态硬盘的电脑，“擦除空闲空间” 的功能是没有作用的。不过，除此之外其他的功能如擦除痕迹和日志等都可以正常使用。

打开程序第一眼就能看见清洁器的图标，在清洁器图标的右边也能看到两个标签，一个是运行系统 (Windows 或 Mac OSX)，另一个是应用程序。

在 Windows (或 Mac OSX) 的下方点选所有的框，这些是在您运行这个程序时会被安全删除的所有不同类型的信息。

在Win10版本中这个菜单的最下方是擦除空闲空间的选项（先不要点选这些，特别是如果您用的是SSD固态硬盘的话）。

在应用程序标签下能发现更多的安全删除选项。具体的选项取决于您的电脑中所安装的程序。在这里您可以勾选所有框，不过如果不打算删除个人使用的浏览器痕迹，则可以不点选那个浏览器的框。

或是依照对这个浏览器的具体需求点选。（比如可以删除浏览器历史纪录，但是不删除已保存的登录信息）。

请注意：如果您的加密空间（硬盘）在启动 CCleaner 时是开启/加载的，那这个驱动器清单中也会显示出来，没有必要选中加密空间，一般情况就只需要选通常的C盘（系统盘）即可。

Win10版本 “工具” 选项下还有一个驱动器擦除器的标签，这个功能是在不用运行整个清洁器的情况下，仅擦除空闲空间 —— 也就是那些本来应该被删掉了的旧文件。请记得点选 “仅剩余空间”，否则电脑里面所有现存的数据也会被删掉。

现在已经完成了设置，可以先试着运行一次。回到清洁器标签下，点击分析。在快速的分析后，会显示哪些数据会被删除，点击运行清洁器删除这些文件。

按照目前上面的步骤设置， 清洁器内勾选了擦除空闲空间选项，这会花费很长时间。如果您只打算清理操作系统的痕迹或浏览器的上网活动痕迹等，可以再回到清洁器的选项内取消勾选擦除空闲空间选项，重新分析。

如果开启分析时没有关闭已打开的 word 文档、相关的程序或浏览器，会被要求先关闭它们，否则 CCleaner 无法清理。

[image] [image]

关于手机安全

您肯定已经知道了这个道理：手机从来都不安全。如果您有担心、或在需要提高安全性的情况下，都不要信赖手机。关机没有用，只要您的电池还在手机里，您就仍然可以被追踪到。

如果您尚未了解这点，可以从下面看到。

延伸：https://iyouport.substack.com/p/b0e?utm_source=publication-search

延伸：https://iyouport.substack.com/p/00a?utm_source=publication-search

延伸：https://iyouport.substack.com/p/-snowden?utm_source=publication-search

[image]

如果您已经是政府的眼中钉，当然就有更多的方式令他们设法连接您的手机，浏览您的文件、截屏等等。如今做到这件事非常容易，并不需要成为一个职业黑客。

由于这些威胁，您的手机在通常情况下应该仅仅作为一个通讯设备，而不是一个小型的工作电脑。

千万不要用手机下载或存储敏感的文件、文档和照片。彻底的从手机中删除文件是非常困难的， 因此，绝对不要用手机存储（哪怕只是暂时存储）任何工作文件。

至于中间人攻击，那就更常见了，比如众所周知的黄貂鱼，在大型集会/抗议现场警察经常使用这种方法来监视和追捕参与者，他们甚至将黄貂鱼放在飞机上一次性监控成千上万部手机。

[image]

返回：威胁矩阵 - 专题 [image]黄貂鱼

最后，除了这些因为手机本身的功能带来的威胁之外，那些通过手机下载的App也能允许同样类型的连接，**App**甚至更容易带来威胁。

要当心您安装的程序，要清楚地意识到任何中国的公司对中国用户来说都是危险的，因为警方能直接连接到这些公司和他们的服务，这些公司也不会在警方需要的情况下保护您。

准确说，所有寡头公司都不会在被警察和间谍要求的情况下保护您 —— 被硅谷出卖的吹哨人被判处50年监禁，延伸：https://iyouport.substack.com/p/8ba?utm_source=publication-search。

如果您必须使用这些寡头公司的服务，建议将它们单独放在一个特定的设备上，该设备中不应该存在任何对您来说重要的内容。而您的敏感工作需要使用另一台设备，此设备上不应该有这些寡头公司的服务。

[image]

返回：选择工具可参见本站专题 工具-Tools

“我的手机被窃听了吗”

在以前，要找出电话有没有被窃听是件挺容易的事，如果您的电话线被窃听，通常很容易听见重复的喀喇声，或是手机里能听见不规则的干扰噪音。

但现在，更多的窃听都是通过隐藏的 **App** 进行的，更像是黑客而不是传统的电话窃听。不管怎样，传统的电话窃听也在继续的被广泛使用，于是，有一些事项是您需要注意的。

通常来说，如果您的电话线被监听了，它会发出一些噪音，因为这条线被别的窃听者分接了。如果您小时候家里是那种一条电话线被分接了好几个电话的情况，您会知道如果您在通话时家里其他的人拿起了另一个电话，您会很明显听到电话里噪音背景的改变。

所以，要了解自己的电话是否有被窃听，应该要注意在您打电话给固定的某个人时听筒里的正常噪音是怎样的。如果您发现噪音的类型有变，就需要引起注意了。

不管怎样，打电话给不同的人和地点都会有些许不同的噪音，所以您要用一个特定的人和电话来试，看看是否发现什么变化，典型的声响有：

- 重复地喀喇声
- 稳定的噪音干扰
- 尖锐的嗡嗡声，测试的时候确保不要靠近其他电子设备（比如

电视、路由器、电脑等），否则可能会有干扰

如果您的电话是通过手机**App**或后台进程被窃听的，而不是通过电话线的分接您你可以通过以下这些特点来分辨：

- 随机的短消息、包括随机的字符和数字等 (监听软件内不小心流出消息的 bug) ：

- 超长的大量电池消耗

- 突然跳出广告

- 手机用起来慢、卡和不稳定

- 流量使用增多

- 手机过热

[image] [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

如果您使用手机，请注意

和电脑不一样，手机无法有效的保障里面的东西。尽管您已经加密过（现在大部分的手机都是自动加密的），但也没有比这更高端的方法了。

尤其是要考虑，如果您被警方带走他们强迫您交出手机的解锁密码时，怎么办。

[image]

返回：[image]如果您的手机被盗了或被警察抢走了，怎么办

返回：[image]保护安卓手机免受警察的抢夺

返回：[image]如果你被迫解锁手机，应该怎么做

由于手机缺乏多层保护，加上经常性的使用App连接服务，而不是使用浏览器（也无法彻底清除手机上网痕迹），如果您被迫交出解锁密码，警察就不仅仅是能进入您的手机，而是手机内所安装的所有App服务，以及那些近期使用浏览器上网遗留的内容。他们可以用您的手机作为后门。

不要让他们用手机威胁您的安全 —— 也就是不要将手机当成您的工作电脑。

[image]

返回：[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证

简单说，绝不要存储任何敏感文件在手机里，也不要把手机当作文件转移的工具，更不要用手机进入任何您已经在电脑中使用的敏感操作相关的服务。

您的手机可以是非常高效的通讯工具。关键是应该将手机仅仅用于这个目的，而不是任何其他功能。

要想实现这个唯一目的，必须使用安全的应用程序 —— 能自动销毁会话的应用程序，防止外人进入您的手机后从历史记录中挖到对您不利的信息。端对端的加密聊天程序结合自动销毁功能，就是您判断是否值得使用的基本标准。

中断通讯

中断通讯（Going dark）指的是将手机任何类型的数据传输都切断，

这是唯一能确保手机不会对您造成不利的方式。

如果您正在进行一个私密的会议，要确保没有被监听，中断通讯是唯一的解决办法。

同样，如果您不希望被摄像头偷偷记录，或是被他人知道您的地理位置，都应该让手机中断通讯。

中断的方法有几种，最简单的方式就是开启飞行模式，让手机停止发送网络传输（手机跟信号塔窃窃私语的过程）、Wi-Fi传输、还有蓝牙。

这个方法也有弱点，那就是可能在您不知道的情况下手机内某个App的数据传输被启用了 (只要您的手机被列为目标就能被暗中启用)。

另一个可能性是，只要GPS为启用状态，所有的地理位置都会被记录下来，一旦关闭飞行模式，地理位置数据就能通过这个App发送出去。

所以，中断通讯的第二种方式是物理中断，即一个非常简单的习惯，就是用法拉第袋或铝锡箔纸。

很多在敏感领域工作的人都会带上几包铝锡箔纸。用两层铝锡箔纸将手机的每个部位包住，就能将传输切断。

这是中断通讯的最好办法。当然法拉第袋也可以，并且不会太引人注意。

如果用铝锡箔纸，将手机用两层铝锡箔包起来，再试着给这个手机打电话、 发信息或邮件，它应该无法收到。如果能收到，就再加一层。总之，如果您打算采用这个方式，就算只是备不时之需，也请记得在使用前先测试一下，看看包几层才够用。

自动同步和云存储

另一个严重的手机安全威胁是很多的服务都会自动登录。这些App通常和在浏览器上的服务相比都只有比较简单的界面。但是，进入服务通常都是不需要输入密码的。

只要进入到您的手机就表示进入了里面安装的所有服务，千万别低估它的威胁。所以，不要安装一般通过电脑中的敏感工作浏览器进入服务的应用程序。

也不要在工作电脑和手机上同时使用云存储服务或其他的线上服务，最多使用分开的账户和服务。比方说您坚持要使用云存储，那就在工作的电脑上用 Google drive，在手机里使用另外的如 Dropbox 或 OneDrive 存储。也就是保持您的工作电脑和手机使用的服务完全分开。

因此安全的关键是限制手机的使用方式，将手机看作是一个最简单的通讯设备，除了通讯外不用于任何其他目的。不要用手机搜集重要的资料、更不要用手机下载文件和存储重要敏感文件。

[image]

关于地理位置追踪的提醒

要知道,如果您非常迫切的希望躲避追踪，也就是已经被警察、国安局的人跟上了，那种情况下单单让手机 “切断通讯” 是解决不了问题的。

您的车子会自动被一路上的监视摄像头记录下每一个动向，您使用的银行储蓄卡或信用卡、任何用您的名字注册的卡，都能被当作地理位置追踪的入口。朋友发布的您的照片也能给出拍照的时间和地理位置，这些都很容易被自动分析识别出。所以只要是有人想要追踪你的位置，这些资讯就足够了。

[image]

返回：在威胁矩阵中查看上述状态的描述及应对方式 [image]隐姓埋名

另方面，长时间的 “切断通讯” 几乎是不太可能的，甚至是短期的也非常困难，除非您准备好了大量的现金和交通工具等等。现在大型商场的普通监视摄像头都能快速的识别出脸部的轮廓。

手机是通过独有的识别码来辨认的，一个来自手机硬盘本身，另一个来自SIM卡。这个码叫做 IMEI (手机) 和 IMSI (SIM卡) 。这些号码是由手机塔和手机服务商注册的，比如中国电信。

您无法隐藏或改变这些独有的识别码，如果您的手机号码已经被恶意者掌握，那他们就很有可能至少知道了您的IMSI码，如果您的手机被没收，警察就能知道您的IMEI码并找到您存储的数据。

这样，您在过去很长的一段时期拨过的号码、去过的地方、数据的使用等等都能被找出来。

再次强调，手机是一个很大的威胁，不应该用于任何敏感的工作目的。

也就是说，如果您已经成为了被跟踪的目标，上面提到的多种方法都能被采用为进行追踪的方法，所以绝不要让自己陷入被追踪的情形，工作很重要，但是您的安全必须放在首位。

[image]

返回：[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

如果 …… 怎么办

尽管您已经很清楚保障手机安全的困难性，但难免可能需要用到手机浏览器搜索资料、用浏览器登录邮箱或账户、或是用手机储存文件和

数据的时候，请作出以下预防。

⛔

只要使用浏览器，都必须确保先进入浏览器的设置区域，保证密码没有被保存，所有的表单自动填充功能都设置为“不允许”，在使用结束后，浏览器设置里选择“清除数据”。

当然，使用Tor是更好的。

如果不小心在手机里存储了任何文件或数据，安装一个擦除程序，在移除或删除了文件和数据后运行这个程序。

但是请注意，通常这个方法并不像在电脑中那样有效，只能对付一些很简易的取证方法。

针对安卓手机的清除工具是 **Secure Eraser**，苹果的是 **iShredder** (仅限英文版) 。也有其他的类似 App 可选。如果您的手机有SD卡，则需要确保在SD卡和手机的内部硬盘都运行了“擦除空闲空间”程序。

这只是一点补救。总之，最好是不要用手机做重要的操作。

[image]
[image]

为最坏的情况做准备，迎接最好的结果如何在敌对环境中保护自己 S02E04

[image] 关键词	团队 威胁响应 威胁模型 援救 预防性
[image] 关联	[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
[image] 创建时间	2025年4月16日
[image] **Description**	教材

这里是S02系列最后一集，将介绍一些操作步骤，这些操作对您未来的安全具有重要作用。

- Table of Contents

  步骤**1**：您可能面临的威胁是什么
  步骤**2**：您需要什么样的援助
  步骤**3**：指派一名您足够信任的、风险级别足够低的“紧急联络人”
  预备材料
  最后

[image]

步骤1：您可能面临的威胁是什么

描述出您可能会面临的潜在威胁，威胁您的人是基于何种目的？

比如，您是一名公民调查人员，是否有可能因为调查和报道一个敏感事件而导致短期被拘留？或者您的资料被没收、被警察追踪到您的消息来源？或者更严重的逮捕或指控令您无法继续工作? ……

或者，您正在参加一个新的反抗组织被警方发现了吗？如果您并不是该组织的领导人，警察可能会如何利用您挖到该组织领导人的身份？您所拥有的哪些信息容易遭受这种利用？如果拒绝与警方合作，您还有哪些方法能帮助脱身？……

[image]

您可以使用S01系列教材中的习题： [image]S01整体安全 - 总章节：前线安防入门课

不同的威胁类型需要不同的准备工作。您需要清楚地知道，您所做的是哪一类行动、或者和哪个人一起工作最有可能提高您所面临的风险？是您所掌握的真相令您面临风险，还是您正在调查的方向非常敏感？

一旦你清楚自己的行为可能招致的报复，这样就便于识别可能性的报复来源了。

不要夸大。一定要对镇压环境有切实的了解和认识。夸大的推测和猜想只会让状况更混乱。

您是否清楚谁最有可能是加害者（当地政府？警察？国安？私人维稳服务？地头蛇？）；您是否知道如果他们采取对您不利的行动，可能会使用什么方式、或者何种指控？……

请列出这些问题的答案，越全面越好，这样才能便于在有需要的情况下提供迅速的援助。

[image]

步骤2：您需要什么样的援助

基于上面各种问题，您已经分析了自身的安全状况，您认为万一出现危险，什么样的援助是您会需要的？在达到某种事态下，您是否认为受到国际媒体的关注是必要的？如果是，以什么方式？

比如一旦被拘留，您是否认为只有在超过一周之后再让国际社会发声为好，还是希望国内的社交媒体关注，或不需要媒体关注而是更愿意得到低调的外交或联合国的援助？再或者，如果您对同伴很有信心的话，利用逮捕的机会推进行动升级？

[image]

返回：[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

明白这些不同的交涉在不同的情况下有不同的作用很重要，您应该与您信任的同事聊聊这些选择，因为他们可能会在危难之时成为帮你说话的人。

除此之外，有其他形式的援助需求吗？

您是否有家人依赖于您的经济来源？当你被拘留或强迫失踪的情况下会需要到一些援助的，具体是哪方面的援助，经济、医药、学费或租房等？

另外，如果被拘留，甚至更糟的状况，您是否需要法律援助？是否有任何具体的法律需求？

在什么情况下你可能会放弃指派自己的律师的权利？你是否已经有了在最需要的时候可以帮你辩护的律师？如果有的话，他/她是谁？权利组织可以如何联系到您的律师？他是否已经有了你的委托书？

如果这些考量您都已经有了答案，您应该写下一份无论如何都要自己指派律师的说明（或录制视频），明确列出在任何情况下，您都不会接受一个官派律师，并且将这份说明交给不止一个您最信任的朋友或同事。

[image]

步骤3：指派一名您足够信任的、风险级别足够低的“紧急联络人”

您的紧急联络人会负责保存您提供的这些信息，在有事发生的时候将它们分享给能帮助您的人。

以上提到的所有这些材料都会交给这位安全联络人，这个人应该足够明确在出事时他应该怎么做。

还要指派一位在有需要的时候能够签署律师委托书的家庭成员。在选择之前先想一想，因为大多数家属在事发后一开始都会很迟疑，他们不知道在这种情形下该如何去应对，而且有时候警方也会骚扰或拘留当事人的家人以作报复和威胁，所以，确保在选择家庭成员前先和他们商量一下，让家人明白可能面临的风险。

最好选一个理解您的工作的家人，告诉他，一旦有事发生，让他不要迟疑地签署委托书。将您的安全联络人和这位可以签委托书的家人的联系方式互相交换，让他们彼此知道对方。

如上，如果您不得不实名工作或者出现在敏感的现场，您需要委派的可信的联络人需要是持续匿名工作的人，此人应该安全意识足够好，尤其是足够理解和支持您的工作。

在此之前，您与这位联络人的联系应该足够保密，以避免被当局连锅端。

以下是一个清单，可以作为您准备所有资料的指南 —— 不论您是录制视频，还是把他们写下来，都需要包括这些内容。如果录制视频，请记得保存好完整的元数据，以防止当权者狡辩。

1. 个人简介。

2. 详述您自己和您的工作 ，尽量包括可能招致打击报复的主要活动的具体日期，这点尤其能表明警方对你采取的措施是由于对您从事的敏感工作的报复，这对于外界对您个人的协助作用很大。

3. 已经承诺提供法律援助的指派律师联系信息 (最好是写一个简介)。

4. 紧急联络人的联系信息 (最好是写一个简介)。

5. 已指派的签署委托书的家庭成员的联系信息 (最好是写一个简介)。

6. 任何相关朋友和家人的联系方式 (最好是写一个简介)。

7. 任何您认识的记者和外交官、以及其他您觉得会参与援助的人的联系信息（最好是写一个简介）。

8. 一篇带有联系方式的相关同事或工作机构的概述 (这一条可能会带来额外的保护能力以及威胁识别价值)。

9. 准备几张在公众或媒体声援需要时可以采用的照片，您将有在媒体上的形象主控权。

[image]

预备材料

预备的材料是在万一您被拘留或被逮捕的情况下将会公布的东西，也要提前特别说明：这些材料您希望以什么形式、在什么时候、如何公

开。

请参考如下范例，录制几个短视频应该会很有帮助。

要准备哪些预备材料完全取决于您自己，要基于您的敏感工作和您预想中可能面临的威胁而定。

比如：

1、被强迫认罪现象已经很普遍。比如桂民海，一个瑞典籍公民，被从泰国劫持到中国，在他的被迫认罪视频中他被要求说他“不希望得到瑞典政府的任何外交协助”，以及他希望放弃自己的瑞典国籍。

假如他预先已经录制好了一个视频，强调如果自己出现在中国，都是因为被跨国绑架（他并没有去中国的有效证件），如果他声称永远不会放弃他的瑞典国际或拒绝外交协助，那将是一个非常有力的反击，同时也会增加外界对此案的关注度，因而增加援助程度。

2、很多人权人士被带走后被不允许与家人和律师见面或通讯，警方声称是这些人权人士 “自己说” 他们不想要自己的律师，而要用政府指定的律师。

如果此人已经有一个提前录好的视频，清晰的声明他永远也不会放弃自己指派律师的权利，永远也不会接受一个政府指定的律师，当局的暗中操纵就会失败。

3、如果您大概知道警方会从您工作的哪一方面入手对付您，您可以预先录制一个视频说明这份工作是怎么样的、为什么完全合法或者只有增益没有伤害？ 如果您之前因为工作有被威胁或警告过， 将这些受迫害的信息也记录下来。

4、如果您认为警方可能指控您非法组织NGO工作，或指控您金钱上的疏忽或贪污？那您可能有必要将财务报告等资料复制下来发给您的安全联络人，这样也能应对此类指控。

重要提示：如果您提供的档案发生了任何改变，比如地址、安全联络人的联系方式、家庭状况和您的工作，特别是在您的安全威胁有了阶段性的改变的情况下，这个文档应该及时更新您的最新状态，保留变更记录，您也应该重新发送新的版本给安全联络人。

[image]

最后

希望您可以顺利开展工作，永远不会遇到这种危机时刻；但是做好准备，将在很大程度上帮助您应对威胁。

当局的手段在不断进化中，万一您操作失误而暴露身份，您必须能有PlanB方案。这是安全策划的重要部分之一。

如果您被您的朋友选为紧急联络人，您需要和对方协商一套合理的策略，本文可作为参考，您也可以根据自己的环境更具体地添加内容。

感谢学习！

[image]
[image]

S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

[image] 关键词	个人 免追踪 反侦察 威胁响应 自助自检
[image] 关联	[image]数字技术限制和最佳实践；[image]计算机和移动设备取证；分身
[image] 创建时间	2025年4月17日
[image] **Description**	教材

隐藏是一种维持生存的方式。隐藏是一条保留我们自己、直到我们准备好走向光明的道路。

隐藏是一种对于独立的要求，从他人那里独立出来，从我们对自己的错误观念中独立出来，从一种让我们完全安全、需求完全被满足，因此完全被控制的妄想和执念中独立出来。

—— 大卫·怀特

📌

不要任人宰杀，不要任凭操纵。一个新上市的**AI**软件就能导致如此多人主动奉献出一大把致命的个人隐私数据，这类**21**世纪的奴隶制悲惨故事不该发生在本项目的用户身上。

想要获得自由，首先就要学会识别陷阱。

看清那些附着、缠绕、穿透在整个社会躯干上的统治爪牙。

学会逃脱控制，您就是唯一的成功者。

S03系列将尽可能采取简单易懂的描述方法，通过为您展现这个世界被隐藏的真相，以帮助更深刻领会防卫的重要性，并由此提升生存能力。

[image]

[image]

Notes: 重点是学习防御思路和原理，而不是学习工具。包括本站内收纳的工具，都不是无限保值的，随时会有新的更好的解决方案诞生。而防御思路和原理不会有太大变化。

本系列教材的知识点覆盖本站点多个专题栏目，比如操作安全性、行动安全性、技术直觉、自我照护等。但我们将它们放到一起，成为一套带有原理简述和技巧提示的数字安全防御基本思考方式，面向所有关心人身安全、人权自由的人们，不论学习者目前和曾经是否加入过高风险行动。

也因此，S03系列一定程度上也可作为本站其他多个专题栏目的索引——在您关注的相应话题中，从标注色块连接到本站相关内容（“返回”）、以及站外相关内容（“延伸”）。

示例：

□

延伸：https://medium.com/@iyouport/%E5%8F%AF%E6%80%9C%E6%AD%A3%E4%B9%89%E6%B2%A1%E6%9C%89%E9%92%B1-d3bec8596c6c

[image]

返回

换言，本系列教材服务于：

1. 经常情况下必需使用数字方式进行有保密需求的行动的学习者 —— 包括前线社区长期从事幕后工作的联络人、援助组、应急响应小组等；也可以在对上述成员的培训工作中采取。

1. 任何对隐私安全和自卫防御感兴趣的数字技术用户，尤其是初学者。

众所周知，在零日武器“世界大战”的环境下，游戏规则被掌握在最疯狂的权势阶级手中，间谍软件越来越便宜、监视技术越来越发达和深入 …… 这种情况下很容易让人产生数字安全虚无主义的情绪。安全性虚无主义认为，数字攻击已经变得如此复杂，以至于没有什么可以防止它们发生的，也无法削弱其影响。这种结论是绝对错误的。

虚无主义正中恶意者的下怀，他们最希望看到的就是目标不再试图保护自己。即便是最强大的以色列间谍软件，也仍然有办法抵御，尤其是您完全可以通过培养安全操作和数字卫生习惯以最大程度上减小攻击面。

采取有效防御措施所需的两个小基础是：了解为什么要这样做 - 意识到隐藏的环境风险；对比不同解决方案，并能够从中选取最适合自己的 - 了解相关的技术原理。本系列将用简单的方法从常识层面讲述这两个小基础。

希望S03教材能为您积累一些底气。

最后，本系列整体倾向于低技术性解决方案；且无阶梯，您可以从任何一集开始。

列表

[image] 在不自由中创造自己的自由：变得难以被追踪的简单方法 S03E01

[image] 构建防御直觉是生存的基本功：变得难以被追踪的简单方法 S03E02

[image] 与S先生共度美好一天-变得难以被追踪的简单方法 S03E03：反取证技巧

[image] 保持零信任 - 变得难以被追踪的简单方法 S03E04

[image] 少即是多：变得难以被追踪的简单方法 S03E05

[image] 大保健应该成为习惯：变得难以被追踪的简单方法S03E06

[image] 在雷达下低飞：变得难以被追踪的简单方法 S03E07

[image] 到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

[image] 8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09

[image]
[image]

在不自由中创造自己的自由：变得难以被追踪的简单方法 S03E01

[image] 关键词	个人 威胁模型 技术直觉 操作安全性 数据最小化 社交媒体 自卫
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月18日
[image] Description	教材

隐私保护是什么？或者说防御是什么？是懦弱吗？是被动？并不是。如果你能在不自由的世界里为自己和同道营造一片自由空间，你活着这件事本身，就是反抗。

- Table of Contents
强制性隐私限制
您需要亲自动手帮助自己变得难以被追踪
卫星不间断地监视着您
但是社交媒体也是如此…
隐私策略，技术和程序
那么您应该怎么做？
1）本地备份。
2）异地备份。
3）在线备份。
低技术安全性：规避和匿名提示

“应对一个不自由世界的唯一方法就是让自己变得自由，以至于你的

存在本身就是一种有力的反抗。” —— Albert Camus

[image]

强制性隐私限制

每年的1月28日是国际数据隐私日，其实这个“日”挺扯蛋的，它容易让人产生误解，似乎只有在那一天或一周内隐私才是有价值的东西。肯定不是这样。

每一天都应该是隐私日，尤其是在如今这个史无前例的大规模间谍时代。

互联网人的在线隐私几乎不存在，并且每况愈下。在监视资本主义的世界里，几乎每天都能看到新的联网技术旨在收集用户的数据，并且该产品或 App 只是粗略地制定了所谓的隐私权政策和服务条款，只为了证明把我们每个人的数据货币化的合理性。

这一切是如此荒谬，没有人应该接受它作为现实。但人们依旧没能联合起来抵抗，可见的时间内很可能无法终结监视资本主义和政府的间谍行为。

于是倡导者开始致力于教会人们自己保护自己。

您需要亲自动手帮助自己变得难以被追踪

其实看剧都能学到一些东西。比如美剧《Mr. Robot》里面的虚构人物艾略特·奥尔德森，观众可以跟他学到很多难以被追踪的知识。

延伸：https://start.me/w/xqP8Ew

1、艾略特总能保持一种健康的偏执状态，这种心态能迫使一个人主动考虑安全性的问题 —— 强迫自己思考如何躲避追踪。

[image]

2、艾略特竭尽全力隐藏自己的研究，使用的方法就是隐写术，将其文件秘密地嵌入.mp3音乐专辑里；以便一旦有人发现它们，也不会被怀疑其中是否包含了隐藏的文件。

[image]

返回：在本站 “工具” 专题中搜索 “隐写”，以查找相关工具

3、艾略特的操作安全意识（**OpSec**）很强，这意味着他没有俗话说的“沉船”的纰漏；他不会随意向自己不认识的或不信任的人提供任何信息。

[image]

返回：[image]这些使用暗网的人是如何被抓到的？: 总结教训

返回：[image]他们如何抓捕说真话的人？灾难和教训

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

4、艾略特知道如何在网上保持匿名，并且擅长信息搜集 —— 信息收集是决胜的根基，但必须在操作安全的基础上，否则就是陷阱。

□

延伸：信息搜集 - 开源情报 https://start.me/w/bbk9Bo

5、艾略特不使用任何社交媒体；他知道所有社交媒体都是坑。

[image]

返回：[image]社交媒体上的行动主义安全性:框架手册

返回：[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

返回：[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗

6、艾略特用一条胶带覆盖了笔记本电脑网络摄像头，以防止其他黑客监视他。这种极简的方法如今应该已经被大规模普及了。

7、艾略特并没有束缚自己的大量物资，尽管物资与可追溯性几乎没有直接的关系，但是，您生活中的牵挂越多，就越难以快速脱身 —— 而在任何保护性行动中，时间都是生命线。

事实上在这部剧中，您还可以从其他角色示例中汲取灵感和技巧；不管是攻还是防。

很多有用的技巧、隐私和人身安全策略，您会注意到它们的 —— 从互联网到物联网、从诱导到操纵，几乎都涉及，也许您希望尝试一下。

以上列举的不是全部。本系列内容将尽可能涉及得更全面些 —— 即作为互联网世界中的人，您最有可能遇到的危险。更详细说明请参见总章节。

[image]

卫星不间断地监视着您

卫星技术已经开始变得更便宜，全球各地的公司和政府机构都在努力将侦察卫星部署到近地轨道（LEO）外太空。

“美国联邦法规将商业卫星拍摄的图像的分辨率限制为25厘米或大约男人鞋子的长度（军事间谍卫星可以捕获更细粒度的图像）”

众所周知政府可以随时随地监视你，并且现在商业观测卫星已经填满了整个天空。一些拥有卫星的公司正在出售长达**90**秒的“高清视频片段”。

一家名为 EarthNow 的公司表示，将提供“连续实时”监控，“延迟时间短至大约一秒钟……”，这已经对现实生活中的个人隐私构成了巨大的威胁。

这些人正在出售绝对会被滥用的技术。现在来不及担心数十亿的闭路电视摄像头和连接家庭WiFi监视器了，绕轨道运行的卫星可以昼夜监视你。最糟糕的是，你完全无能为力。

但是社交媒体也是如此…

我们分析过 Netflix 的纪录片“The Great Hack”是个洗地作品，它将监视资本主义的本质转嫁到一家第三方公司身上 —— 并且还拒绝承认该公司（**Cambridge Analytica**）本身就是英国国防部的一部分。

延伸：为什么说剑桥分析公司不是重点 https://iyouport.substack.com/p/9ab?utm_source=publication-search

延伸：剑桥分析公司不仅仅是一家公司，而是政府国防机构的一部

分，这就是为什么该公司可以迅速通过解散来避免被深究，并且，迅速组成新公司：https://iyouport.substack.com/p/pr?utm_source=publication-search

不过可以肯定的是，这部片子对于很多仍在鼓里的人来说依旧是有点用，至少它介绍了剑桥分析公司如何收集数据、并使用其数据操纵选举。

[image]

返回：

返回：

并且选举操纵只是冰山顶上的一块小石头而已。

它也足够能提醒，这个世界上有如此多的贪婪之徒，他们可以为了钱做任何事。那就是监视资本主义的本性。

这也是为什么说您必须也只能立即采取措施保护自己，否则必定会以各种想不到的方式成为受害者。

您无法防止数据收集公司的数据泄露，但是您可以尝试控制被收集的数据类型，从而使监视资本家更加困难。

如果直到如今，互联网上依旧能找到您的真实身份或重要的身份线索，那就是非常危险的；任何了解 “开源情报” 追踪的人都不会对此表示怀疑；还有您的家人，尤其是无辜的孩子，您需要保护他们所有人。

以下是自我检查的方法。这里提供的工具可能有一部分过时了，但基本思路不变。

延伸：https://web.archive.org/web/20190925173253/https://www.iyouport.org/%E8%87%AA%E6%88%91%E4%BA%BA%E8%82%89/

延伸：https://web.archive.org/web/20190925173256/https://www.iyouport.org/%E7%A4%BE%E4%BA%A4%E5%AA%92%E4%BD%93%E6%83%85%E6%8A%A5%E5%92%8C%E5%8F%8D%E6%83%85%E6%8A%A5%E5%9F%BA%E6%9C%AC%E5%B7%A5%E5%85%B7%E6%89%8B%E5%86%8C%EF%BC%9A%E8%87%AA%E6%88%91%E4%BA%BA%E8%82%89%EF%BC%882/

请向您的孩子解释监视资本主义世界幕后发生的事，帮助孩子有意识地控制在互联网上泄漏的敏感个人信息。

各地正在加紧制作隐私法案，但您需要知道，立法者基本都不懂技术，他们很容易被寡头企业忽悠，其结果是，即便立法管制也很难保护您。因为仅仅强调隐私是不够的。

以下是部分解释：

延伸：https://web.archive.org/web/20191029121133/https://www.iyouport.org/%E4%BB%A5%E9%9A%90%E7%A7%81%E4%B8%BA%E7%9B%AE%E7%9A%84%E7%9A%84%E6%96%97%E4%BA%89%E5%A6%82%E4%BD%95%E8%AE%A9%E4%BD%A0%E5%8F%98%E6%88%90%E4%BA%86%E7%9B%91%E8%A7%86%E7%9A%84%E7%9B%9F%E5%8F%8B/

延伸：https://web.archive.org/web/20200519034636/https://www.iyouport.org/%E9%9A%90%E7%A7%81%E6%B3%95%E6%A1%88%E7%AE%A1%E4%B8%8D%E4%BD%8F-facebook-%E5%92%8C-google%EF%BC%8C%E6%80%8E%E4%B9%88%E5%8A%9E/

延伸：https://web.archive.org/web/20201020231028/https://www.iyouport.org/%E4%B8%BA%E4%BB%80%E4%B9%88%E9%9A%90%E7%A7%81%E4%BF%9D%E6%8A%A4%E6%B3%95%E8%A7%84%E5%B9%B6%E6%B2%A1%E8%83%BD%E8%B5%B7%E5%88%B0%E4%BD%9C%E7%94%A8%EF%BC%9F/

延伸：https://web.archive.org/web/20200514081756/https://www.iyouport.org/%E4%B8%BA%E4%BB%80%E4%B9%88%E8%AF%B4%E6%AC%A7%E6%B4%B2%E6%96%B0%E6%B3%95%E8%A7%84%E5%8F%8D%E8%80%8C%E4%BC%9A%E5%8A%A0%E5%BC%BA-facebook-%E5%92%8Cgoogle-%E7%9A%84%E9%9C%B8%E6%9D%83%EF%BC%9F/

[image]

隐私策略，技术和程序

毫无疑问。云不是您的朋友，它是监视的盟友。

请记住，您作为用户，对云的控制为零，这尤其意味着您不应该信任云。

它本身就可能很脆弱，您甚至都不知道。您只会在数据泄露的新闻登上头条之后、或者在您的身份被盗并且银行帐户被清空之后，才开始毛骨悚然。

我们介绍过无数保护隐私的个人技术方法，但是，如果您的信息已经上传到任何一种 “云”，那么所有这些自检清理的防御方法都不再有效 —— 您删不掉的。

Google、Dropbox、Amazon 或 Microsoft 的管理员才有权那么做。就像 MySpace 的管理员滥用其“霸王”工具来监视社交媒体平台的用

户一样，每个云服务提供商和社交媒体的管理员也都具有执行相同操作的工具。

您永远不会知道这些公司何时会与执法机构或政府间谍合作，共享您的个人云存储文件或社交媒体内容 —— 中国用户更应该明白这个道理，苹果把密钥都交给中国政府了。

□

延伸：https://iyouport.substack.com/p/10a?utm_source=publication-search

延伸：https://iyouport.substack.com/p/548?utm_source=publication-search

那么您应该怎么做？

这里是最基本的。

1）本地备份。

将数据本地备份到硬盘驱动器（HDD）（为此几乎不需要额外的工作）。

如果您在计算机系统上安装了分区或一个以上的HDD，则将主HDD设置为固态硬盘（512GB），其中的数据主要存储在使用全盘加密（FDE）保护的HDD上，使用诸如 Veracrypt，BitLocker 之类的东西，或 dm-crypt / cryptsetup 或 Linux 机器的 Linux 统一密钥设置（LUKS）。

如果辅助驱动器（例如，CPU D：\ 或其他）具有足够的大小（即 2–3TB），并且已正确配置了备份任务计划，则可以用来存储C：\自动

数据备份，在一段时间（例如6到12个月）后，擦除旧的数据备份。

关于全盘加密，参见以下的用例和注意事项。

[image]

返回：[image]当你手握真相：最基本的防护知识

返回：威胁矩阵 [image]网络取证

返回：[image]攻击加密系统的多种形式和防御方法

返回：[image]如何安全地留住证据：给真相的记录者一些技术技巧建议

返回：[image]来自人身的威胁：如何在敌对环境中保护自己 S02E01

2）异地备份。

每月备份在一个断开连接的外部硬盘驱动器上；将外部硬盘安全地存储在法拉第袋子中也是好主意，以防止高海拔电磁脉冲（HEMP）的影响。

3）在线备份。

首先应使用 Veracrypt 或其他某种加密应用程序对数据进行加密，然后再使用传输层安全性协议（TLS）v.1.3 将数据安全地上传到信誉良好的平台。

为了确保没有人可以窥探您的数据，除了云服务提供商使用的DaR加密之外，您还需要使用您自己的加密（即 Veracrypt，BitLocker，LUKS）对其进行了双重加密。

不建议您创建自制的加密，而是使用自由开源软件（FOSS）软件（例如 Veracrypt）来加密文件。

低技术安全性：规避和匿名提示

威胁建模非常重要 —— S01教材中有详细流程和习题。您要提防的人是谁、什么东西最值得您保护、您的对手有什么样的技术能力、您有哪些优势能抵御对手？等等，需要保持清晰，且保持更新。

尤其是，采取对抗性思维模式是有益的，像敌人那样去思考、站在对手的视角上看自己，以便更好地监视自己的薄弱环节，及时弥补，以保护资产和信息。

隐私是一项艰苦的工作，这个集中化的互联网上的默认隐私状态为零！您必须努力做到这一点，以实现某种相对安全性、并保持住它。

安全永远是相对的，只要是有足够庞大的资源和技能的对手，所有技巧和技术都可能被击败。但是，任何一种专注的保护工作都能给您带来回报，只要您抢在前面，就能给对手制造足够大的难度。

[image]

零信任。始终验证。不留痕迹。 —— 这是您应该拥有的健康的偏执。

[image]
[image]

构建防御直觉是生存的基本功：变得难以被追踪的简单方法 S03E02

[image] 关键词	加密 对抗性思考方式 技术直觉 防御 零信任
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月19日
[image] **Description**	教材

构建防御直觉需要一定程度的基础知识；幸运的是仅仅是基础知识就可以帮您有效地获得安全，您并不需要去理解技术深层的逻辑。

- Table of Contents

  当无法避免的时候必需保持警惕
  在反加密战争中强调防御直觉
  在各方面保持警惕从来都没错
  在现实中保持防御直觉
  采取对抗性思考方式避免受害

“变得难以被追踪” 就是要成为自己，而不是害怕成为自己。要安心地完成自己的心愿，而不必担惊受怕。

请不要误会任何关于匿名、分身术、角色扮演技巧中所强调的保护性措施 —— 它们都是为了保全您成为自己的自由。

因为没有任何人能在被监视的状态下成为自己 —— 只有您成功摆脱了监视状态，你才是你。

[image]

这里是关于在现实世界和在线环境中索回您的基本人权所需要的东西，您将学习如何控制哪些类型的信息、以及如何向他人显示可被观察和跟踪的信息量。

并不是说要您放弃所有技术，而只是放弃某些技术方面 —— 这些方面一直在监视、收集、窃取和出售您的个人信息，这些信息本来只属于您自己，而不是其他任何人。掌握它就是您的基本人权。

请记住，这是一个由富人控制的、并通过奴役普通人仅仅令富人受益的世界。获得自由的第一步就是摆脱它。

社会上贫富之间的鸿沟正在迅速加剧。富人控制着社会的几乎所有方面，但他们不想让您知道。他们与我们所有其他人所遵循的司法体系不同。

我们中很多人日复一日地挣扎以维持生计，为养活自己和家人，而富人生下来就继承了数百万美元甚至数十亿美元，他们以欺诈剥削穷人和中产阶级为生。他们的钱不是用来吃喝的，而是游戏政治，通过推进那些能令他们自己受益的立法以加固阶级地位。

富人有能力做出选择，不把自己的数据和注意力作为产品出售。穷人和中产阶级就没有同样的资源来实现这个目标。技术曾经是为富人服务的。而现在，富人正在付钱以避免技术。

[image]

当无法避免的时候必需保持警惕

虽然大量用户会看到应用程序的使用完全无害的一面，但是，政府及其情报机构将应用程序或应用程序商店视为为网络间谍工具 —— 将

恶意代码注入应用程序的机会。

[image]

返回：

长期以来，随着新技术的不断出现，基本人权不断受到践踏；尽管如此，那些砖家给出的解决方案似乎非常简单—— “别用就行了”；但是，事实上并不是那么简单的。

例如，当雇主要求雇员在其智能手机上安装指定的多因素身份验证（MFA）应用程序以连接到公司的网络为提高数据安全性时，该雇员被迫做出决定是关于究竟是“交出”手机，还是放弃这份工作。

对于某些人来说，这就是放弃的理由。已经有大量的证据证明雇主在其提供的计算机系统上监视雇员的一举一动，你甚至无法打官司，因为法律认为这些情况通常不存在“对个人隐私的合理期望” —— 因为你接受了雇主提供的电脑，因为你不得不养活自己。

延伸：https://iyouport.substack.com/p/-facebook?utm_source=publication-search

延伸：https://iyouport.substack.com/p/26d?utm_source=publication-search

延伸：https://iyouport.substack.com/p/252?utm_source=publication-search

多因素身份验证应用程序本身通常不是问题，因为大多数操作都是良性的，它们不侵犯隐私。但就像在智能手机上安装 Facebook 应用程序那样，它收集来自其他 Apps 的数据、电话设备详细信息、以及网络浏览历史记录，以便与 Facebook 共享。

对于注重隐私的个人来说，这是一个主要问题。但对于其他可能不知道或无动于衷的人来说，也许不是。这完全取决于您对个人权利的关注程度。

这里的建议是：请注意您在公司网络上访问的所有网站和应用程序。您的雇主极有可能正在监视此类活动，在某些极端情况下，它可能会被用来对您进行绩效评估，甚至成为终止雇佣合同的理由。

并且不要使用公司电子设备做任何与私人有关的事，也不要把自己的手机连接到公司网络。

这就是防御直觉：当您看不到老大哥在哪的时候，您必须假定它无处不在，从而全方面的保持警惕。

在反加密战争中强调防御直觉

> “鼓励互联网公司为其产品和服务建立合法的访问解决方案，包括加密的数据， 以便执法部门和主管部门在数字证据被删除或托管在国外的*IT*服务器上或被加密的情况下，依旧能顺利访问…… ”— *G7 France, 2019*

反加密的战争在全球如火如荼，政府和执法机构为迫使 Big Tech 创建后门以破解加密想出来各种歪点子。以下只是仅举几例：

延伸：https://web.archive.org/web/20200928054332/https://www.iyouport.org/%E5%8F%8D%E5%8A%A0%E5%AF%86%E7%9A%84%E6%88%98%E4%BA%89%E6%AD%A3%E5%9C%A8%E5%8D%87%E7%BA%A7%EF%BC%9A%E7%BE%8E%E5%9B%BD%E3%80%81%E8%8B%B1%E5%9B%BD%E5%92%8C%E6%BE%B3%E5%A4%A7%E5%88%A9/

延伸：https://web.archive.org/web/20200302073657/https://www.iyouport.org/facebook%E6%89%BE%E5%88%B0%E4%BA%86%E8%AE%A9%E7%AB%AF%E5%AF%B9%E7%AB%AF%E5%8A%A0%E5%AF%86%E5%A4%B1%E8%B4%A5%E7%9A%84%E6%96%B9%E6%B3%95/

延伸：https://web.archive.org/web/20200927185343/https://www.iyouport.org/%E5%85%B3%E4%BA%8E%E5%B9%BD%E7%81%B5%E7%94%A8%E6%88%B7%E5%92%8C%E5%BC%80%E8%A3%86%E8%A3%A4/

延伸：https://iyouport.substack.com/p/--041?utm_source=publication-search

这是一场持续不断的战斗，在反抗者令其变得更好之前，它只会变得更糟。

澳大利亚政府官员通过了一项法律，要求公司为情报和执法机构提供加密后门，这绝对是对数字隐私的公然侵犯，并且完全表明缺乏对基本人权的尊重。

所有这一切恶行都以所谓的“国家安全”的名义进行。“国家安全”只是政权稳固的委婉说法，并且它暗示其中包含“人民的利益”，事实上哪里都没有人民的利益，人民只是必需付出的代价。

您可以打赌，全世界其他国家的政府都在密切关注这项法律，并将尝试通过类似的立法 —— 而不仅仅是中国。

如果在您的地区任何加密通讯都无法使用、所有翻墙工具都失败了，那就试试隐写术吧，也许是可行的出路。 BACK 在本站“工具”专题中搜索“隐写”，以查找可用的工具。

[image]

在各方面保持警惕从来都没错

您不应该在看到刀子后才想到血，那就为时已晚了。正如本节的主题所强调的，在各方面保持一种警觉，至关重要。

对富人的警觉、对寡头企业的警觉、对各种 便利性诱惑 的警觉，当立法没有听取并充分思考你的意见时，保持对法律的警觉。

到目前为止，苹果公司是大型科技公司中喊隐私喊得最响的一个，尽管单单这点并不足以让您想为他们的产品支付同类其他产品2至3倍的价格。

但您应该了解：

延伸：https://iyouport.substack.com/p/-apple-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/578?utm_source=publication-search

所有这些寡头技术公司都在不断地监视跟踪，这不是秘密，这就是监视资本主义的本质。您必需自己保护自己，作为普通人，我们很难指望任何人。

[image]

返回：[image]一句话安全须知：记住这些句子，以简单地优化您的安全性

香港的抗议活动一度成为全球热点，从某种意义上说，抗议者采取了多种预防措施来保护自己的真实身份，他们戴着口罩面罩、使用现

金，并将其通信限制在可提供端到端加密的应用程序中。

这绝不仅仅是香港的故事，它应该是全球反抗者的基本须知，因为如今没有任何一个国家的政权不会采取这些监视迫害方式瞄准活动家。

返回：在本站的“ 行动安全性 ”专题中看到详细教程。

显而易见，中国官员会使用社交媒体情报和监控录像加面部识别软件来揭示抗议者的真实身份。并将这些被识别出的个人添加到中国政府维护的“黑名单”中，并极有可能成为重点监视目标，从此再也没有安宁。

不必怀疑，所有政府都保留着类似的黑名单，尤其是政治异议、活动家、记者、边缘社区、人权维护者、人权律师 ……

你真的应该庆幸还有这些勇敢的香港抗议者与老大哥作斗争。

[image]

当使用 Match.com、OkCupid、PlentyOfFish 或 Tinder 等约会网站时，您正在与一些直接捏住你的人权的公司共享最私密的数据。

亲密的聊天消息、药物使用习惯、收入水平、性偏好、简历、宗教观点、社会偏好 ……等等，这些只是在这些约会网站上收集的数据类型的几个例子而已。

这可不仅仅是被收集的问题。就像 Ashley Madison（成人网站）在2015年遭到黑客入侵，被泄露的数据类型是高度个人化的，非常危险。之所以被泄漏正是因为一直不断的收集。

约会网站只是一个例子，在这点上，任何网站和应用程序都一样。

没有人会喜欢这样的事发生在自己身上。防止这种情况发生的唯一方法是尽力限制您在网上发布的信息。

这不是一个完美的策略，但这是您为保护自己能做的最好的事之一。

在现实中保持防御直觉

也许是时候考虑不再使用民宿了（比如Airbnb），预订酒店房间相比下更好点，相比下风险稍低。

[image]

返回：[image]查找隐藏的摄像头和防入侵：把移动设备变成监测仪

如上述提示，每一次住店都要这样做；因为秘密监视是如此的普遍，防御直觉必须假定任何时候都有可能存在危险。尤其是当您准备进行敏感的会面时。

如今信息技术世界中普遍使用的电子产品或硬件使普通消费者对任何一种技术的工作方式都难以了解。人们可能知道自己购买的设备中芯片装在哪，但是，如果把它们拆开，敢说绝大多数人都无法从中挑出不应该存在的东西。

有时，后门隐藏在设备的固件代码中，这可以使监视者远程监视设备。在过去十年左右的时间里，信息安全社区已经看到了越来越多的硬件后门植入示例，通常被称为供应链攻击。

□

延伸：https://web.archive.org/web/20201027152916/https://www.iyouport.org/%E4%B8%80%E5%91%A8%E5%86%85%E4%B8%A4%E8%B5%B7%E4%B%9B%E5%BA%94%E9%93%BE%E6%94%BB%E5%87%BB%EF%BC%9A%E4%B8%A5%E9%87%8D%E7%9A%84%E7%8A%B6%E5%86%B5%E5%B7%B2%E7%BB%8F%E4%B8%8D%E5%AE%B9%E5%B0%8F%E8%A7%86/

延伸：https://web.archive.org/web/20201027154235/https://www.iyouport.org/supermicro-%E7%94%B5%E8%B7%AF%E6%9D%BF%E6%9C%AC%E8%BA%AB%E5%B0%B1-bug-%E7%BC%A0%E8%BA%AB%EF%BC%8C%E9%82%A3%E4%B9%88%E4%B8%BA%E4%BB%80%E4%B9%88%E4%B8%AD%E5%9B%BD%E6%94%BB%E5%87%BB%E8%80%85%E8%BF%98/

如果没有正确的技能和知识来检查固件代码以及主板或芯片组的外观，这种类型的威胁将是巨大的，而且几乎是无法阻止的。

民族国家多年来一直使用供应链攻击在手机、计算机和所有类型的电子设备中植入后门。芯片级恶意软件可以更改操作系统（OS）而不会留下痕迹，就像在视频游戏中打开“上帝模式”一样。

这类间谍活动有一整个地下市场，其逻辑就像灰帽子向政府出售零日漏洞以获取巨额资金那样。这种事一直都在发生，人们只是不知道它的程度如何罢了。

延伸：https://medium.com/@iyouport/%E5%8F%AF%E6%80%9C%E6%AD%A3%E4%B9%89%E6%B2%A1%E6%9C%89%E9%92%B1-d3bec8596c6c

延伸：

如今已经在芯片组中发现了多个引人注目的漏洞，例如 Meltdown、Spectre 和 ZombieLoad 等等，利用这些漏洞，攻击者就可以获得对系统的root级访问权限。

可怕的是，其中一些芯片缺陷是无法修补的，这意味着它们将存在相当长的一段时间，直到最终被新硬件取代。

保护您的电子设备免受此类缺陷影响的唯一方法是定期检查制造商的

网站，以获取需要应用于该设备的补丁程序更新。

否则设备可能会面临各种攻击，如果设备连接到互联网，则可以远程执行这些攻击。

另外，请谨慎购买某些类型的电子产品。大多数物联网（**IoT**）设备在安全性和隐私控制方面的设计都非常差。

[image]

返回：[image]你家冰箱如何作为呈堂证供？

延伸：https://iyouport.substack.com/p/lr--a49?utm_source=publication-search

购买之前需要考虑的因素包括数据应用、安全设计和安全硬件、以及制造过程中的透明度和可见性 —— 而不是制造商宣传的有多大的内存、几个摄像头、拍照效果多牛逼 ，他们只是想让你掏钱并转移你的注意力远离最重要的事。

[image]

采取对抗性思考方式避免受害

现实中几乎经常是温柔而正义的人不断成为狡猾的掠食者、骗子和罪犯所设置的陷阱的受害者。

绝不是说要您放弃温柔正义，而是说，您很有必要努力把自己的精神思想和身体打造成坚不可摧的堡垒。

走这条路永远不会太迟，但是无疑，您将需要迎接各种考验。

必须知道每个人都有弱点，这是坏人的主要目标。就像一只烫手的烧水壶，你要把它拿起来、控制住它，就需要抓住壶的把手 —— 目标人固有的弱点对于操纵者来说就是那个把手。

相反，如果您要防御各种侵害，就需要让自己的“把手”不可见。中文里“小辫子”一词在此格外形象。

就像窃贼那样，网络掠食者会充分搜集并分析您的一切在线行为，并观察可公开获得的关于您的每个细节，以确定他们是否可以利用您的任何漏洞。

由于公开的已经太多了，对于您隐藏的或不公开的内容，他们完全可以推断出大概。这就是为什么说每个人都必须时刻意识到自己放在互联网上的都是些什么 —— 这就是防御直觉。

似乎依旧有很多人不甚了解究竟什么东西是危险的 —— 了解这点是防御的关键。我们来举个例子：一个人在社交网络发布了一张照片，显示为某个当日举行的会议/活动的现场，并随附 “今天天气真好，是和家人一起出行的好日子”。大多数人会认为这样的信息 “不敏感”；但是人们没能通过恶意行为者的视角来观察它。只有这样做才能真正有效地防御。

这需要练习。

现在我们就来试试看，通过上面这条内容你能知道什么？

- 此目标人似乎正在全家外出中，所以TA家中可能没有人；
- 迅速查找目标人的其他社交媒体平台账户，以搜寻此人可能的住址；
- 通过简单的搜索立刻能知道，目标人提及的会议/活动的召开和结束时间；

- 通过该活动的性质你能知道目标人的偏好；

- 通过照片中阴影的角度你能知道拍摄的大致时间，以对比发布时间判断同步程度；如果拍摄时间和发布时间之间间隔多小时，这将说明更多细节；

- 仔细看照片，其中有哪些特征：画面中有出现电子设备吗？能看出品牌型号吗？有徽标/胸牌吗？能否判断其他参与者的身份？胸牌是门禁卡吗？这意味着安全设施方面的信息；其中多数人穿的是什么样的衣服？这可以判断其阶层和品味偏好 …… 所有这一切都是实施社交工程攻击和黑客入侵的关键信息。

- 还可以有更多。

也许作为您，和家人一起出行参加活动是一件乐事，但是，对于攻击者来说，您的愉快假日已经变成了明确的攻击入口。

类似的状况几乎铺天盖地，这就是为什么我们要强调 —— 不要通过互联网讲述关于你自己和家人朋友的任何信息。

您需要防备的不只是警察和政府间谍，恶意行为者在社会上到处都是，他们能干出任何你可能想都想不到的事。因为他们整天都在琢磨这些东西。

只要恶意者能发现您的PII，例如 您的全名、卡号、出生日期、手机号和家庭住址，那么他们就能窃取您的身份，并以您的名义开放信用额度，劫持你的SIM，不要等钱没了时再表示惊讶。

人类最大的弱点就是总会下意识地认为最糟糕的事不会发生在自己身上，这是一种心理防御机制，是你的大脑在试图把问题简化从而避免紧张焦虑的自然能力。但是，它可能很有危害性，正是它导致人们在看到他人的教训时将自己放在旁观者的角度上，错过了吸取教训的机会。也正因此，一模一样的恶行手段会不断重演，而且每次都能有效。

✂

学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。你不需要亲自被考糊了才能学到东西，要知道一直不断有人被考糊，他们的教训应该成为更多人的知识。

并不是说要你草木皆兵地生活，防御直觉指的是：您需要了解当前每个领域有可能发生哪些恶行，并随时为最糟糕的状况做好准备。

你准备得越好，最糟糕的状况就越不容易发生。

[image]
[image]

与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧

[image] 关键词	分身 反取证 反追踪 数字取证 示范
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月21日
[image] **Description**	教材

有多少追踪方法，就有多少反追踪方法。

- Table of Contents

  数字取证
  反取证技术与对策
  1、数据隐藏
  2、反取证擦除
  3、足迹混淆

[image]

> 孙子曰：微乎微乎，至于无形；神乎神乎，至于无声，故能为敌之司命。

S先生乘坐1986年的老吉普车CJ-7来到公共图书馆。

作为一个务实低调的人，他更喜欢可靠的老古董车子，这类汽车不依

靠计算机芯片来运行，并且速度也足够快。

延伸：https://web.archive.org/web/20200228095225/https://www.iyouport.org/%E5%B0%8F%E5%BF%83%E4%BD%A0%E7%9A%84%E6%B1%BD%E8%BD%A6%E5%8F%98%E6%88%90%E9%97%B4%E8%B0%8D%EF%BC%9A%E5%A6%82%E4%BD%95%E4%BB%8E%E8%81%94%E7%BD%91%E6%B1%BD%E8%BD%A6%E4%B8%AD%E5%88%A0%E9%99%A4%E4%B8%AA/

延伸：https://iyouport.substack.com/p/cbf?utm_source=publication-search

延伸：https://iyouport.substack.com/p/d21?utm_source=publication-search

延伸：https://iyouport.substack.com/p/150?utm_source=publication-search

S先生喜欢书，他每周要去图书馆两次，以便在公用计算机上检查他的电子邮件，并交换他已经阅读过的书籍选择新的书。

图书馆的停车场在建筑物的屋顶上装有闭路电视（CCTV）摄像头，可以捕捉包括S先生在内的所有进出的车辆，但由于S先生的车子很脏、车牌上沾满了泥土，所以无法很好地读取车牌。

不过要知道，在某些国家，车牌不干净是非法的。所以，避免车牌阅读器监视的方法应该不是遮盖，而是欺骗。比如这样：

📌

延伸：https://web.archive.org/web/20200718080928/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E6%84%9A%E5%BC%84%E8%87%AA%E5%8A%A8%E8%BD

%A6%E7%89%8C%E9%98%85%E8%AF%BB%E5%99%A8%EF%BC%9F/

随时都可能有新方法出现。您只需要在自我保护方面多花点心思。

[image]

不止车子，摄像头还捕获了S先生走进图书馆正门的情景 —— 他的脸，但由于S先生戴着红色球帽、帽沿上带有微型的**LED**灯，并用白色字母和墨镜模糊了他的脸部轮廓，可以欺骗面部识别算法。

还有很多有效的做法，具体见下面：

□

延伸：https://iyouport.substack.com/p/3e6?utm_source=publication-search

再一次，这些解决方案一直都在更新中。

S先生是活动家，他是抵抗地方和中央政府权力超限的社会运动的一部分。他珍视自己的隐私，并且不喜欢被政府收集有关他生活习惯的任何信息，例如他从图书馆借出的书。

除球帽外，S先生的衣服没有任何特征，吸睛度压到最低。

这很重要。而且不止衣服，请注意下面这些提示：

[image]

S先生将他的书放在车上，走过去坐在一台提供免费互联网访问的公用计算机前。

这是他经常访问的几个图书馆之一，S先生已经确定了所有闭路电视

监视器的位置，并选择了一台其显示屏不在监视器视野范围内的可用计算机。

请注意这是一整套技巧，您首先需要知道的是您在监视者眼里是什么样：

[image]

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

S先生在图书馆计算机上打开了默认的浏览器，恰好是 Internet Explorer 版本11（即 11.285.17134.0），因为该计算机仍在运行 Windows 7。在公共场合这是非常普遍的现象。

这个图书馆几年来一直没有获得必要的资金来升级其15台公共计算机。

IE版本11就像Web浏览器的老旧汽车。它存在漏洞，容易受到多种未修补漏洞的攻击，并且由于自2016年1月12日起不再受到 Microsoft 的支持而完全无奈。

[image] *IE 11 Common Vulnerabilities & Exposures; courtesy of the MITRE Corporation*

如果管理员尚未禁用此功能，S先生的第一步就是清除浏览器历史记录、缓存和**cookie**。

通常，公共图书馆的计算机都处于锁定状态，因此它们受到严格限制，以防止人们不当地使用它们。

接下来，S先生导航到 Gmail，并创建了一个一次性电子邮件账户

（garbage2434234@gmail.com），专门用于注册 “Hide My Ass” 虚拟专用网络（VPN）的7天免费试用。

关于如此使用安全的一次性电子邮件账户：

[image]

返回工具推荐：[image]临时/一次性电子邮件服务选项

不要直接使用公共计算机登陆您的私人电子邮件，也不要直接录入任何真实的私人信息；但必须知道，容易隐藏身份的最佳选择恰恰是公用计算机 —— 如果您已经被瞄准了并正在计划撤退路线，它就是个好选项。前提是您能做到S先生这样。从下方进入S04完美隐身教程，查看具体建议。

[image]

返回：[image]S04完美隐身-总章节：机智是重要实力

一旦建立了可随时丢弃的电子邮件帐户，S先生就将假信息输入HideMyAss VPN 7天试用网页注册中，以包括他较早前用现金购买的预付礼品卡中的付款信息。

如果您不方便用现金买礼品卡怎么办呢？别忘了以下小技巧：

□

延伸：https://iyouport.substack.com/p/5-f54?utm_source=publication-search

[image]

返回工具：[image]生成假的信用卡资料使注册更安全

由于这是一张礼品卡，S先生将伪造的地址以及他新建立的一次性电

子邮件地址输入到地址字段中。

他尝试打开命令提示符，发现他没有打开命令提示符应用的权限。S先生熟悉Windows操作系统，于是搜索 PowerShell 以获得完全访问。

S先生键入“ **ipconfig / all**”，并记下了他正在使用的图书馆计算机当前未受保护的以太网适配器IPv4地址。然后使PowerShell窗口保持打开状态

[image] *PowerShell example of the “ipconfig /all” command*

同时，信用卡注册成功完成，S先生可以选择将VPN软件下载到计算机。他能够将程序文件下载到桌面，但是很快发现，他被阻止启动程序可执行文件（.exe）。

S先生收到一条错误消息，指出此操作需要提升的权限。

S先生决定尝试猜测管理员凭据，然后右键单击可执行程序文件，选择“以管理员身份运行”选项。

S先生仅几次尝试便成功猜出了密码。原来是 P@ssW0rd123……看起来管理员是个很懒的家伙。

[image]

在本站“工具”专题中搜索“密码”，以找到密码安全和保管的解决方案。

然后，他继续安装自己下载到计算机桌面上的 HideMyAss VPN 程序。

这花费了大约5分钟的时间，现在S先生可以从公共图书馆的计算机上匿名上网了。

[image] *HideMyAss Virtual Private Network (VPN) service; image*

courtesy of HideMyAss.com

一旦VPN运行正常，S先生通过cmd打开命令行窗口输入 ipconfig /all 验证了新IP地址，然后重新启动 Internet Explorer 11并继续打开其实际的电子邮件，ProtonMail 帐户（ProtonMail提供自己的VPN服务，但需付费，出于本示例的目的，选择突出显示 HideMyAss）。

ProtonMail 帐户为“ JackerCrack911@protonmail.com” —— 请注意，他的真实身份从来都不是其电子邮件地址的一部分。

现在，他还知道管理员密码，这将使他在用完后更容易擦除踪迹。

S先生检查了他的电子邮件和个人银行业务站点、以及其他一些站点。如果他没能在公共图书馆计算机上使用VPN，浏览这些敏感网站可能是危险的。

当然，更好的方法是**Tails**，装在**USB**里挂在钥匙上。

[image]

[image]

在本站“工具”专题中搜索“VPN”，以找到相关解决方案。

[image]

许多人也许认为，拔掉 USB之后不会留下任何痕迹。实际上，**Windows** 会把可移动设备视为永久客人。每次连接的 **USB** 存储设备都会在注册表中被记录下来，包括其制造商、产品名称、序列号以及上次查看的时间。这使得在取证分析期间最容易调查的内部威胁之一就是 **USB** 活动。

即使文件被删除、USB驱动器已经消失很久，系统仍然会记住它。Windows 会将设备注册为 USBSTOR，给它分配一个驱动器字母，并在系统日志中记录安装事件。

数字取证调查者可通过关联这些痕迹来证明特定**USB**设备曾连接至特

定机器，并通常能确定该设备是否用于数据传输。

本案例不会“吸引”数字取证调查的注意。但如果您的实际情况有可能招致调查，请谨慎。

在网上冲浪大约20分钟后，S先生关闭了网络浏览器。但在关闭之前，S先生仔细清除了浏览器的搜索历史记录、清除cookie和缓存。

他还删除了 **Pagefile.sys**、**swap** 和 **thumb** 文件的内容，因此，如果没有高级**IT**取证软件工具和技术，否则无法轻松恢复其浏览历史记录。

[image]

返回本站攻防矩阵模块 - 关于“取证”的页面 [image] 法医取证

- [image]数字取证

S先生随后终止了VPN连接并卸载了 HideMyAss VPN 软件。

他从 C:\ProgramFiles 目录中删除程序文件，然后在 Windows 搜索栏中键入“ regedit”，然后选择“以管理员身份运行”。

他输入适当的管理员帐户登录凭据，该凭据之前已被他成功地猜中，并且 “注册表编辑器”模块打开。

接下来，S先生导航到 “Computer\HKEY_LOCAL_MACHINE\SOFTWARE” 他找到并删除了 “HideMyAssVPN” 软件注册表项。

S先生然后通过在Windows搜索栏中键入“事件查看器”并右键单击该应用并选择 “以管理员身份运行” 来打开Windows事件查看器。

他再次输入管理员帐户登录凭据，然后选择 “Windows日志”、“应用

程序” 选项。然后，他向下滚动以查找由安装 HideMyAssVPN 应用程序和卸载程序所生成的 events。

接下来，由于S先生使用管理员帐户完成了这些操作，因此他将打开安全日志，并仅删除与其操作相关的事件。千万不要删除整个日志哦，那样就是此地无银了。

[image] Windows Event Viewer Application Log example [image]

毋庸置疑，以上是假想事件，尽管所有这些操作都可以执行，但普通用户不一定就能如此成功猜测管理员帐户密码并能够擦除其记录。

如果您感觉此示例过于繁琐、过于详尽、或者过于技术性而难以执行，也并不需要灰心丧气，但这确实表明您可能尚未完全意识到要变得几乎无法被追踪所需要实际努力。

要变得几乎无法追踪并不容易，而且您必须熟悉技术，才能在一定程度上了解计算机系统和网络的运行方式。

您能够在 **Mac** 或 **Linux** 操作系统上执行相同的操作吗？您是否知道在哪里可以找到文件甚至文件的名称是什么？而且您还应该注意到，**VPN**本身有可能存在不安全因素。

[image]

返回：[image]如何检查您的VPN连接是否实际加密

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

延伸：https://iyouport.substack.com/p/vpn?utm_source=publication-search

数字取证

[image] *Hex Editing; Image courtesy of SANS DFIR*

关于数字取证，您只需要知道它大概是什么，以及如何尽可能将损失降至最低，即可。如果您是有一定经验的行动者，可以通过下面的威胁矩阵入口进入该主题。本系列教材对这个部分只做简述。

[image]

返回本站攻防矩阵模块 - 关于“取证”的页面 [image] 法医取证

- [image]数字取证

正如您所知道的，有些方法和工具可用于恢复已删除的文件并从计算机系统和硬件中提取关键信息。

如果调查人员能够确定S先生已下载并安装了 HideMyAss VPN，那么他们还可以获得令该VPN服务提供其日志副本的授权书，作为数字取证调查的一部分，以对他提起诉讼。

在数字追踪方面建议多一些谦虚，即便您已经做了很多，依旧会有很多坑可能您尚未想到，不论是本地计算机、网络上那堆寡头公司、还是ISP，都可能出卖你。

换句话说，一个人永远不可能变得完全无法追踪 —— 但是，您能做到尽可能地难以被追踪。这样就足够甩掉大部分监视者。即消耗战：玩死对手，耗尽他们的财力和精力，你就赢了。

数字取证调查的主要目标是犯罪嫌疑人，而起诉方必须能够证明数字证据来自据称被犯罪嫌疑人使用的计算机，并且数据是精确的比特流副本。

反取证技术与对策

[image] *Anti-Forensics Extended Taxonomy; M. Rogers & the 16th*

想要做到难以被追踪，就要首先认识到。那些知识丰富和经验丰富的IT专业人员 —— 尤其是执法数字取证调查员和情报机构网络分析师 —— 他们拥有各种方法、技术和工具，可以恢复删除的文件，可以跟踪您的在线活动，并帮助挖掘您的真实身份。

易于追踪监视就是这个集中化互联网的本性。不止是专业技术人士，就连普通人也可以做到在一定程度上追踪监视某些目标，熟悉 “开源情报” 调查的任何人都不会怀疑这点。

您需要保持对这一事实的认识，并据此进行操作 —— 这一领域有多致力于取证工具的设计，就有多致力于反取证工具的设计，后者这些工具专门用来打败取证工具。

接下来看一下有哪些可用于帮助实现在线不可追溯性的技术和工具。

1、数据隐藏

隐写术的思考方式有着悠久的历史。在数字时代，您可以通过将机密数据嵌入和加密在其他载体文件中（例如图像、文本、视频和音频文件）来隐藏数据。

[image]

在本站“工具”专题中搜索“隐写”，以找到相关解决方案。

只要找到恰当的隐写应用程序，几乎任何类型的文件都可以用于隐藏数据 —— 有**1100**多种，找到恰当的工具并不难。

相对的，密码术是隐藏数据的另一种方法。当然，总是会建议您在硬盘和电话上使用全盘加密（包括**SD**卡）。但是真的有许多隐藏数据的方法。如下表所示的打包程序和捆绑程序将可执行文件压缩为其他类

型的文件，并将它们绑定在一起，这也使得可执行文件更难被进行逆向工程。

[image] *List of Executable Packers; courtesy of Wikipedia*

Rootkit 就是通过这种方式形成的。 Rootkit 基本上是一种恶意软件，它由“一组程序和代码组成，它们允许在计算机上进行难以检测的root级访问（Donzal，2005年）。”

Rootkit 有时也被警察甚至公司IT部门用于远程访问/监视目的。

由于它们被隐藏并深埋在防病毒软件可能无法扫描的计算机操作系统文件中，并且具有多态性，因此检测非常困难。

通常，rootkit不会像蠕虫一样自我传播。可以通过单击电子邮件或网站上的恶意链接，将Rootkit下载到目标的计算机上，该恶意链接在打开您想查看的链接的同时，也开始悄悄地下载所谓的“dropper”文件。

2、反取证擦除

如果计算机上有您无法找到的敏感信息，可以对计算机进行编程以自动擦除整个操作系统。执行后它将自动开始删除文件，从而使数字取证更加困难（甚至不可能）。

不过，如果您忘记了正确的启动顺序，这也会给您带来麻烦。最好有备份！

如果调查人员注意到了正在发生的事，那么他们也许可以迅速关闭系统，但是至多，他们只能得到部分数据。

反取证擦除工具，例如在 Kali 或 Black Arch Linux OS 发行版中发现的一些工具，SRM、Wipe、Overwrite、DBAN、BCWipe、Eraser，R-Wipe、DiskZapper、Cryptomite 或 Evidence Eliminator，都将能有效删除并覆盖内存使其无法恢复。

基础学习者可以返回S02的相关部分：

[image]

返回：[image]备份和恢复已删除的文件

返回：[image]恢复误删除的数据

返回：[image]彻底卸载

返回：[image]定期清理硬盘

- 再次提升：所有工具都是快速更新换代；唯防御原理不会有根本性变化。请将注意力放在后者。

3、足迹混淆

想象一条狗正在追踪你。狗熟悉你的气味。但如果你用香水、臭鸡蛋、薄荷叶……糊了一身，狗就找不到你了。

混淆就是这样的原理 —— 在网络上植入关于您自己的虚假信息，以使您摆脱追踪者的嗅觉。

从这个意义上讲，它涉及使用复杂的工具来修改有关您的活动的数据。

例如，删除日志、在访问系统或网站时使用袜子木偶身份、故意提供错误信息、使用分身帐户、提供**IP**地址跳跃（**Tor**，**I2P**，**FreeNet**），使用 **Timestomp** 等类似工具修改时间戳、元数据和文件头信息。

关注此部分的学习者可通过以下标注块深入了解。

[image]

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

返回：[image]给活动家的反人肉指南

返回：[image]如何知道有人正在线人肉你？6个简单的方法

返回：[image]袜子木偶 - 分身创建的小技巧

返回：[image]使用Tor保护自己时千万不要做这9件事

如您所见，“变得难以被追踪”比您最初所认为的要困难得多。在此，技术经常不站在您一边。您可以在本站的“技术直觉/技术哲学”专题中看到具体解说。

[image]

返回：[image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

必须强调的是，要变得难以被追踪，首要条件是思考和看待世界的精神成分 —— 您需要知道追踪者的思考方式，然后才是虚拟或网络空间的技术成分。如果您知道如何做的话，就会发现不难做到。

您越是熟练，信心就越足。信心会给您勇气和力量。保持低调，继续让自己成为堡垒的主人。

[image]
[image]

保持零信任 - 变得难以被追踪的简单方法 S03E04

[image]	关键词	国家安全 技术直觉 数据安全 自卫 零信任 高科技镇压
[image]	关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image]	创建时间	2025年4月22日
[image]	**Description**	教材

不要指望法律保护你。能保护你的人只有你自己。

- Table of Contents

  我们绝不是顽固的技术反对者
  别指望法律
  隐身模式：＜**ON**＞
  地堡
  高级持久威胁就在您的后院

本集内容关于最基本的技术自觉，适合初涉安全领域的人权关注者。明确的高风险用户/学习者可绕过本集内容；建议从“威胁知识库”开始。

[image]

我们的主题是 “难以被追踪”，而不是 “免于被追踪”。因为如果想要做到 “免于”，您首先就要做到避免遇到任何监视追踪设备。这在如今是完全不可能做到的。

只要您走出家门，每个角落都隐藏着监视摄像头和注视的眼睛。那么远离城市呆在沙漠里或大草原上似乎就没有监视器了吗？错误。太空中卫星每时每刻都在监视着整个地球上的一切，这些卫星具有令人难以置信的强大变焦能力，可聚焦到1米（即3英尺），并且图像分辨率很高。

政府间谍可以把卫星记录下的一切都拿走。

延伸：https://web.archive.org/web/20200407143856/https://www.iyouport.org/%E4%B8%8A%E5%B8%9D%E4%B9%8B%E7%9C%BC%EF%BC%9A%E4%B8%80%E4%B8%AA%E6%B2%A1%E6%9C%89%E7%A7%98%E5%AF%86%E7%9A%84%E4%B8%96%E7%95%8C%E6%84%8F%E5%91%B3%E7%9D%80%E4%BB%80%E4%B9%88%EF%BC%9F/

延伸：https://web.archive.org/web/20200518224512/https://www.iyouport.org/%E5%8D%AB%E6%98%9F%E5%B7%B2%E7%BB%8F%E5%BC%80%E5%A7%8B%E8%A7%82%E5%AF%9F%E4%BD%A0%E7%9A%84%E6%AF%8F%E4%B8%80%E4%B8%AA%E5%8A%A8%E4%BD%9C/

有时，那些充满敌意的眼睛属于人类，这就是最常用的人力监视 —— 我们目前仍认为当权者不会放弃人力监视，因为它调动灵活、敏感性强、针对性高。它会和各种技术搭配使用，几年内不会被技术所取代。 BACK 在本站“行动安全性”中查看对抗人力跟踪监视的可能方法。

也有时，这些眼睛是监视摄像机的镜头，借此人眼可以远距离观看现场，包括稍后回溯重播视频。

以上仅仅是指户外。

如今越来越多的是，那些充满敌意的眼睛就在您家中 —— 在您的房屋中安装监控摄像头时、在您忘记在电子设备摄像头上贴黑胶布时、当您安装的所谓“智能”家居存在您不知道的隐藏摄像机时……

不仅是看，还包括记录：这些东西正在作为将您定罪的证据。

[image]

返回：[image]你家冰箱如何作为呈堂证供？

就如类似总部位于意大利的 Hacking Team 这类公司，专门设计各种黑客工具出售给世界各地的政府和执法机构，使他们能够入侵目标受害者的手机、计算机甚至家庭Wi-Fi监控系统；以色列NSO有多恐怖就更不用说了。您可以从下面的列表中查看相关内容。

延伸：https://start.me/w/8LRjvQ

延伸：https://start.me/w/OaLzjO

那些家用监视摄像机可以对您很不利，尤其是通过Wi-Fi连接时。也许您认为监视器对于家庭安全来说不是个坏主意，但是，请要小心它们会曝光您。

对此感兴趣吗？可以参见下面这个工具。亲手玩一下，您会理解为什么。

延伸：https://web.archive.org/web/20191002015052/https://github.com/jakejarvis/awesome-shodan-queries/blob/master/readme.md#intel-active-management-cve-2017-5689--

监视在21世纪是无处不在的，这已经没有任何疑问。如果您居住在美国、中国、英国、印度、俄罗斯 …… 等国家，那么你肯定知道，您的政府始终会认为隐私人权远不如所谓的国家安全更重要。

几乎每天都有新闻曝光政府如何践踏公民的隐私人权、一个新的大规

模数据泄露事件、或另一个配置错误的 Amazon Web Server（AWS）被盗。

是的，变得“难以被追踪“ —— 也就是保护您的基本人权 —— 已经变得越来越难。虽然这并不意味着完全不可能，您应该尽可能尝试、尽快地尝试保护自己。尝试活得像个人。

[image]

我们绝不是顽固的技术反对者

很多技术都是双刃刀，可以用于善恶两种目的；就如面部识别，在政府间谍手里被用来追踪镇压抗议者，在公民社会手中用来寻找失踪的儿童和老人。

□

延伸：在政府手中时 https://iyouport.substack.com/p/386?utm_source=publication-search

延伸：在公民手中时 https://iyouport.substack.com/p/--e37?utm_source=publication-search

再如AI和大数据，在政府手中就是民主终结者，在公民手中就是直接行动的武器。

□

延伸：在政府手中时 https://iyouport.substack.com/p/--786?utm_source=publication-search & https://iyouport.substack.com/p/--310?utm_source=publication-search

延伸：在公民手中时 https://web.archive.org/web/20200929200818/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E8%BF%8E%E6%8E%A5%E6%9B

%B4%E5%A4%9A%E7%9A%84%E5%B7%B4%E6%8B%BF
%E9%A9%AC%E6%96%87%E4%BB%B6%EF%BC%9F/

这就是为什么我们强调：只有技术是民主的，社会才能是民主的。公民掌握技术以构建自己想要的社会，这是非暴力直接行动的最佳方式。

当人们不断被当权者欺骗的时候；当不断有人被抓捕却对抓人手段一无所知的时候；当信息战狂热将民主逼上死角的时候 …… 公民掌握侦查的能力就是改变世界的直接行动。

同样，没有任何当权者不撒谎，因为权力就构建在谎言之上。他们几乎隐秘一切，同时只让你看到他们希望你看到的东西。这种情况下公民发起的透明度革命就是亲手打造自己想要的世界。

这需要强大的技术能力，如您所知 —— 异议不是反抗，反抗不是直接行动。异议可能不需要技术技能（如果您不担心被捕的话），但反抗肯定需要，直接行动则非常需要、而且是更丰富的技术技能才能满足。

简单说，如果您和您的组织尚未精通，那就无法真的开始。请随时记得这是21世纪智能镇压时代。

[image]

别指望法律

生活在数字时代您需要能随时记得，您眼前的几乎一切都被永久性在线了，您的一切都在被收集、被分析、被储存、被出售 …… 被用来指控您、作为把您扔进监狱的证据。

即便如此，目前为止仍然很少有人选择反对这种做法。

例如，最简单的，除非您同意允许 Cookie，否则许多网站将不允许您

访问。再比如，用Tor保护自己的人被大量热门站点所排斥，被认为“可疑”，被视为“互联网二等公民”。

这就是监视资本主义的世界 —— 它阻止你逃离地狱。

寡头技术公司、电话服务公司、和互联网服务提供商（ISP）受益于宽松的甚至完全不存在的法律，完全不受阻碍地继续运作这个地狱。您可能很难依赖法律来保护您，因为立法者是权贵，他们从这个地狱生态中受益。

几乎没有任何人可以阻止这种情况的继续，因为互联网法规仍然是狂野西部，并且具有严重的地理限制 —— 记得吗，硅谷寡头的口头禅“我们在遵守当地法律”。不论是帮助追捕异议人士还是将密钥交给政府，使用的都是这个借口。

但您完全可以做的是，努力使自己成为捍卫自己人权的卫士。

众所周知在现实中您的身份的至少一部分被视为公共资产，正因此，在在线情况下您应该积极搜索自己的任何信息并及时删除或尝试最小化其在线状态。这就是我们强调的自我人肉和大清洗。

[image]

返回：[image]自我人肉

再次，这不是一件容易事，您需要特别的努力；但它真的有效，而且有可能是唯一有效的方法 —— 让自己成为你的对手最头疼的威胁，变得难以被追踪。

隐身模式：＜**ON**＞

防御主机 (Bastion host) 指的是经过专门设计和配置以抵抗攻击的专用计算机。该计算机通常承载单个应用程序，例如代理服务器，并且

所有其他服务都将被删除或限制以减少对计算机的威胁。

在其两边都有防火墙（面向Internet和面向组织）并且所有不必要的服务和端口均已删除并关闭。

这是一个比喻。为了变得难以被追踪，您必须努力成为 **Bastion** 的宿主，并将所有不必要的暴露风险最小化。

将这点与日常生活联系起来，意味着您需要至少采取以下行动：

- 从互联网上尽可能删除所有个人身份信息（PII）；
- 冻结您的信用记录档案并设置欺诈警报；
- 与他人做任何交谈时，请注意尽量不要谈及您的个人信息（小心您的 “随口说说” 就会泄漏大量秘密， 在本站的“心理安全”专题中看到关于社交工程的介绍。比如 [image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术” ；
- 尽可能少地使用社交媒体，或者至少要非常小心在线发布的任何信息、照片/视频（避免包含您的家庭住址、车牌、自己的面孔、朋友和家人的面孔等重要信息的照片）；
- 通过使用代理以最大限度地减少外部跟踪暴露；使用加密的电子邮件；或使用隐写术；
- 在出国旅行中，不论是出境还是入境，事先删除所有社交媒体应用程序、加密通信、VPN、文档，之后再重新安装。尤其是出入美国和中国，这点非常重要！

就数字隐私理念而言，当您遇到个人抉择时，使用奥卡姆剃刀作为指南是不错的选择。

因此，如果您曾经遇到过关于数字隐私的多种哲学，并且不知道该选择哪一种时，通常最直接的选择就是不共享您的任何个人数据，或至少选择能保证保护您的隐私并拥有可靠记录的组织。

将所有政府和寡头公司都视为敌人，这是最可靠的认知 —— 任何政府，任何国家的寡头公司 —— 监视资本主义没有国界。

[image]

地堡

世界上真的有专门用于数据存储的安全港，例如 “Cyber Bunker”，人们可以安全地存储自己的数据，而政府间谍和警察无法接近。

他们为海盗湾等组织众多镜像提供托管。也是为什么2019年德国警方冲进特拉本-特拉巴赫附近的一个 Bunker 的数据中心并将其关闭一事引起了巨大的反响。

这些数据托管通常位于国际刑警组织可监视范围之外的国家，且与用户所在国家之间没有引渡条约。

作为个人，您可能不需要将您的个人文件存储在国际防弹地堡里，但是如果您出于某些原因这么做了（比如您正在本国实践透明度革命），那么这样做是绝对有必要的。请准备支付大笔费用，因为它们并不便宜。

□

延伸：https://web.archive.org/web/20200703084001/https://www.iyouport.org/%E6%9C%80%E4%BD%B3%E5%BA%87%E6%8A%A4%E6%89%80%E5%92%8C%E8%B7%A8%E5%9B%BD%E7%BB%B4%E7%A8%B3-%E9%80%8F%E6%98%8E%E5%BA%A6%E9%9D%A9%E5%91%BD%E7%9A%84%E6%9C%AA%E6%9D%A5/

高级持久威胁就在您的后院

众所周知，全球绝大多数政府都希望能够轻松地窥探自己的人民。您也一定知道，全球反加密战争是如何地惊人。

对那些间谍来说，民主自由并不会让他们赚到钱，但维护其主子的权力地位稳固他们就可获得享不尽的富贵。所以，永远不要指望他们任何“良心发现”。

政府只关心如何更轻松地解锁您的加密智能手机、笔记本电脑、读取您的加密通信、以便能把您扔进监狱。

说良心话，宪法和法律中写的如何保护人权的那些字很可能并没什么用，这在很多国家都是如此。比如美国和中国，如果您坚持行使宪法权利阻止非法搜查和扣押，那么您在当局眼中会自动被判有罪，他们会拘留您，并将您带到可以为您的任何设备发布搜查令的法官面前。在下面看到相关调查报告：

延伸：https://iyouport.substack.com/p/lr--093?utm_source=publication-search

如果您拒绝提供密码/ PIN，您可能会被判蔑视罪。可笑吗？并不是。在9/11之后，《第四修正案》的宪法权利基本就作废了。

尽管您已经尽最大努力在网上和现实生活中保持匿名，但随时了解自己面临的挑战仍是至关重要的 —— 随时知道你的政府正在干什么。

延伸：https://iyouport.substack.com/p/--041?utm_source=publication-search

延伸：https://iyouport.substack.com/p/cdc?utm_source=publication-search

这些数据正在由高级计算机系统处理和分析，使用算法使用在语音、视频和数据中搜索任何关键字。比如下面这些 - 还有更多更多：

延伸：https://iyouport.substack.com/p/ibm?utm_source=publication-search

延伸：https://iyouport.substack.com/p/--602?utm_source=publication-search

延伸：https://start.me/w/bbk9po

[image] *The Salt Lake Tribune) An aerial view of the NSA's Utah Data Center in Bluffdale, Utah*

在中国什么样，想必大家心里都明白。但依旧有人认为“如果我没做坏事就没什么可担心的”。是吗？什么是好事什么是坏事你真的知道吗？你不知道，因为你的价值观一文不值，好还是坏的标准永远是由监视者定义的。

那谁来监督监视者呢？

如果仍不能回答上述问题，你就必须保持对任何权势的零信任。

零信任，始终验证 —— 这是基本原则 。

[image]
[image]

少即是多：变得难以被追踪的简单方法 S03E05

[image] 关键词	VM 低技术性 反取证 数字卫生 数字足迹 消费主义 自检 隐写术
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月23日
[image] Description	教材

您不得不牵挂的东西越少，您的行动就越自由。在数字安全领域也是如此：极简主义是一种生存法则。

- Table of Contents
什么是强化
欺骗与谎言
逃避监视的低技术方法
纸和笔
保持安静
上传任何东西之前请三思
BlackArch Linux
黑暗艺术 **L33t**

在这个新十年里，随着技术能力的快速发展，监视资本主义会近一步飞跃，政府、互联网技术公司、以及各种服务公司对你的私密数据的需求量只会越来越高。

从监视资本主义开创的最初，信息就已经取代了黄金和其他所有货

币，成为了新的货币标准 —— 只要有了足够的信息，一个人或组织就可以按照自己的喜好来控制他们想要的任何东西。

[image]

这一切早已不是秘密。 全球各国政府基本都是同样的操纵者，而且已经做了很多年。

□

延伸：https://iyouport.substack.com/p/--786?utm_source=publication-search

延伸：https://iyouport.substack.com/p/lr-2019?utm_source=publication-search

说实话反抗者还是很多的，他们在议会、在法院、在街头、在电脑桌前拼搏。但是，每当一方认为自己在争取隐私的战争中取得了重大胜利时，压迫性技术便会伴随着一种新的方法出现，以此把你打得粉碎。

□

延伸：https://iyouport.substack.com/p/--91a?utm_source=publication-search

监视和反监视就是现实生活中的汤姆和杰瑞，公民人权一直跑在逃亡的路上。我们必须能扭转这个局面。

[image] 《Mr.Robot》台词。 ……重点是最后一句话

什么是强化

您可能已经发现，本系列的前4集都比较简单，它们侧重于从基本面上帮助每个人认识到我们生活的世界中发生的最惨烈的真相。

换句话说，这些是如今每个人都应该熟知的 —— 从熟知开始，才有改变的可能。

第5集希望说明的是，“变得难以被追踪” 并不完全是 “低技术含量” 的问题，而是，您要想到办法使政府间谍和监视资本家的机器变得笨拙，由此才能找到生存能力。

在政府和贪婪的寡头公司眼中，你我这些公民仅仅是纳税人、潜在的选票、满足未来市场销售形式的金钱符号，甚至是敌人 —— 如果您质疑那些权势的话。

简单说，他们只要能保证您不造反、继续源源不断地把钱给他们，此外的一切他们都不会关心。包括您的基本人权和活得像人的尊严。请理解这点。

一次又一次的数据泄漏，一次又一次的侵犯，直到大众媒体已经对灾难习以为常，不再成为 “热点” …… 没错，他们要的就是这个，他们都明确告诉你了：“新常态”。

[image]

一个人可以做些什么才能使自己的个人信息更难以被收集和利用？保持对这个问题的思考至关重要。

要回答这个问题，您需要首先清点与自己有关的所有攻击面，并采取补救措施，以最大程度地降低风险，这取决于您的个人情况、资源和动力。

[image]

这与现实中一样。如果不想挨揍，就必须想办法保持自己的身体健康和活跃，从而增强抵抗力。找警察、找政府、找哥们儿，可能都不如您自己的二头肌更管用。

学习一点防身术是自卫和提高自律的好方法。在心理/精神方面，强

化涉及使您的思想免受有害的社会影响，并防止自己屈从于将您的个人信息自由地拱手于每个渴望喝你的血的当权者和寡头。

[image]

返回：[image]如何从Matrix中醒来

同样，在我们通常称为“网络空间”的信息安全维度中，强化除了其他众多定义外，还涉及为减轻不必要的风险而采取的措施；例如，删除不使用的系统服务、限制应用程序、关闭防火墙上不必要的端口、以及整个操作系统和Web浏览器中更严格的配置设置，等等。

极简主义者将在此拥有明显的优势，即 拥有最少的东西、最少的文件以满足基本的保护、说明、备份、加密、管理 ……

更少的事物意味着更少的攻击面，可以做到强化和防御。

但是，如果您全家用一台电脑，这可能会比较困难。因此，这句话应该说成：请在可能的情况下尽一切办法减少自己的攻击面。

欺骗与谎言

愚蠢地陷入了全球消费主义热潮的群众们不知不觉地变成了羊，并自愿将自己的身家性命无偿提供给了无良的寡头，让这些寡头赚得盘满钵满。

消费主义宣传机器通过新的互联网、电视和广播营销广告来推动这一无休止的消费主义循环，这些广告旨在使消费者将更多的钱花在他们根本不必要的产品上，并在此过程中收集更多的个人信息。

让我们看一个单一的产品，例如 iPhone。

为什么像苹果和三星这样的公司（可以说是整个行业中最大的两家手机制造商）拥有类似的商业模式，每年发布新版本的 iPhone 和 Galaxy S 手机系列？您有没有想过这个问题？

□

延伸：https://web.archive.org/web/20191117103114/https://www.iyouport.org/%E8%8B%B9%E6%9E%9C%E5%8D%96%E7%9A%84%E7%A9%B6%E7%AB%9F%E6%98%AF%E4%BB%80%E4%B9%88%EF%BC%9F%E8%BF%99%E4%B8%AA%E6%97%B6%E4%BB%A3%E6%9C%80%E5%85%B3%E9%94%AE%E7%9A%84%E4%B8%8D%E6%98%AF%E6%8A%80%E6%9C%AF/

至少，这已经在2017年被发现的，并得到了苹果的证实 —— 关于：他们已经放慢了老款 iPhone 的速度。他们想诱使您去买新的。

再一次，少既是多。请不要把您的钱花费在为自己制造危险的事情上。

鉴于当今的手机数量比活人还多，众所周知这并不是一种普遍的看法。但是，我们依旧认为，智能手机可以也应该在某些重要的场合被禁止进入，您肯定知道哪些场合是重要的。

[image]

返回：[image]你的手机如何背叛了民主？

返回：📱 警察如何利用抗议者的手机追踪每个人

返回：[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

并且，与此同时，正是这种永无止境的消费主义和公司贪婪的循环正在破坏地球的自然资源，并将那些“跟不上消费主义进度”的人们沦为二等公民，因为他们“必须拥有最新最好的产品”。

技术曾经是为富人服务的。现在，富人正在付钱以避免技术……

延伸：https://web.archive.org/web/20200519051916/https://www.iyouport.org/%E7%A9%B7%E4%BA%BA%E7%9A%84%E5%B1%8F%E5%B9%95/

现在最重要的是，让更多人意识到发生了什么。让自己摆脱疯狂。政府是监视资本主义体制的最大受益人之一 —— 您在政府的重点监视名单上了吗？别忘了，当权者把公民视为敌人。

[image]

对于某些类型的技术，保持普通的防伪直觉并不是一个坏主意。比如，汽车应该可以被入侵吗？被直接开到警察局门口并熄火？换句话说，这种汽车您真的想要吗？

[image]

返回：[image]构建技术直觉：生存在数字世界必备的本能

不要小看恐怖分子，仔细研究下基地组织在逃避对手的偷袭以及如何避免使用手机和卫星电话方面取得了多么大的成功，能学到很多东西。

基地组织在严峻的偏远环境中运行，但仍在隔离房中使用技术。他们的视频和音频消息总是预先录制并定时，以提供最大的震撼和恐怖效果。到预先录制的消息公开时，操作人员早已无处可寻。

而我们这些人，还在拼命地玩直播 ……

说实话，已经证实基地组织甚至曾使用数字隐写术将没有任何密码保护的作战计划文件放在色情内容里。而那些经常喝茶的人们却对隐写术不以为然……

[image]

在本站“工具”专题中搜索“隐写”，以找到可用的解决方案。

基地组织和伊斯兰国等恐怖组织使用的这些低技术含量的防御措施在逃避侦查方面可以说很有成效，就算受到破坏，也无需花费太多成本即可维护或更换。

不论您想做任何事，或者仅仅希望保住自己的基本人格和尊严，防御技术知识和能力都是您的基础。

衷心地希望所有好人都比坏人更聪明。

请随时记得，只有像敌人一样思考，您才能保护住自己的个人生活，对任何人来说都是如此 —— 开源情报就是这样的练习，帮您站在敌人的角度上认识自己的弱点，以便提前堵住漏洞。

支个招。您可以将隐私概念和技术与节俭、简约和低配的概念和解决方案相结合，进行一些实验，以确定在尽可能少花钱的情况下最能实现所需防御效果的方法；请随时告诉自己，您完全不需要通过拥有更多“事物”使自己的生活变得更加混乱。

门铃是干什么用的？有人来了摁一下提醒你去看猫眼，对吗？所以，您只要买一个能响的东西就行了，真的有必要安装亚马逊的Ring那种东西吗？这是举个例子。

□

延伸：https://iyouport.substack.com/p/e6d?utm_source=publication-search

延伸：https://web.archive.org/web/20200422203218/https://www.iyouport.org/%E4%BA%9A%E9%A9%AC%E9%80%8A%E5%B8%AE%E5%8A%A9%E8%AD%A6%E6%96%B9%E6%9E%84%E5%BB%BA%E4%BA%86%E4%B8%80%E4%B8%AA

%E5%B9%BF%E6%B3%9B%E7%9A%84%E7%9B%91%E6%8E%A7%E7%BD%91%E7%BB%9C/

以下是您可能希望在生活中实施的一些低技术防御选项。很有可能您探索得越深，就越会发现，高科技和低技术的混合方法最有效。

逃避监视的低技术方法

如今，只要您不是生活在生山老林里，只要走出家门，就绝对会遇到一大批监视摄像头。

尽管不可能完全实现匿名，但是，您仍然可以采取一些简单的非技术性的措施来避免监视和 “选择退出系统”。

[image] 上图中提到的东西在这里下载：https://t.me/iyouport/6779

比如，在纽约市，**isee** 应用程序可帮助市民规划出行的最小被监视路径。并非在任何地方都可以使用此功能，但大多数地方您都可以根据来往沿途的监视摄像机数量来确定自己的路线。

这就是直接行动：亲手打造您想要的东西，而不仅仅是乞求当权者拆掉监视器（您知道那会很难）。

当然，上述案例不是最佳的，只是一个例子。尽管有可能迫使当权者继续投资更多的监视器，也没关系，这意味着反抗形成了主动 —— 让您的对手追着您跑，而不再是您永远追着他们的悲惨局面。

上面的下载材料中有更好的行动案例。

戴墨镜和戴棒球帽、LTD灯头盔等等简单的事，就可以帮助破坏面部识别，使监视系统更难以瞄准您，并且可以成为一种有效的迷惑技术。

□

延伸：https://iyouport.substack.com/p/3e6?utm_source=publication-search

对准CCTV摄像机的激光也可以遮挡其视线，但是，如果不能精确执行 …… 结果可能很严重。因为它已经拍到你了。

请注意，在一些国家，比如美国，在街头戴着 LED 灯的球帽是违法的，就像将您的车子开到泥潭里并不违法，但很可能会导致车牌不清晰、不干净。中国怎么样我们不知道，您最好先熟悉一下当地法律，尤其是上面那篇文章。

任何法律都有漏洞，就像软件，所以，合法意味着，只要你能找到漏洞。

苹果公司的乔布斯以其经常利用加利福尼亚法律中的漏洞而闻名。此漏洞如今已被关闭，但在当年，这使他可以在租用的梅赛德斯·奔驰SL55 AMG没有牌照的情况下驾驶，他将在六个月的宽限期结束前将其出手然后换成相同的车型。从2019年开始，在加利福尼亚州购买的所有汽车都将随附DMV颁发的牌照。

想想看，从您走出家门开始，一路上有多少个摄像机？红绿灯路口都有监视器、收费公路上也有摄像机、还有隧道摄像机，它们记录下的一切都被输入了自动牌照读取器（ALPR）中，以及由某些未知的计算机系统处理。

□

延伸：https://iyouport.substack.com/p/9d2?utm_source=publication-search

您需要能找到一条尽可能少地遇到这些东西的路。

反侦察技巧**101**：兜圈子，越复杂越好。如果实在躲不开监视器，那

就不要走那条从出发点到目的地的捷径；在其间兜圈子，让监视者难以察觉您的目的地在哪。

您是否从自动柜员机提款、停下来加油、或从当地的超市买东西？如果这样做了，请再添加一些可以跟踪您的摄像机。

Investigation Discovery（ID）有线电视频道制作了一个名为 “See No Evil” 的节目，其中详细介绍了警察如何使用视频回溯来追踪目标人的方法。您可以看一下。我们一直认为中国应该多做这些研究和介绍，YouTube上的“热门”中文演讲视频基本都没什么价值，这太可惜了。

监视程序的揭露表明，政府间谍从许多主要的互联网服务提供商（ISP）和电信服务提供商手中直接收集用户数据。不要认为这种情况在任何国家会“不一样”，永远不要相信那些公司会重视您的利益，因为控制社会是稳固权力的基本。

延伸：https://iyouport.substack.com/p/8ba?utm_source=publication-search

[image]

纸和笔

先不要笑。

低技术方案 —— 例如使用笔和纸 —— 的妙处在于，它通常便宜得多，并且无需考虑其他任何因素，例如 不必更改密码、不必将通电、不必通过危险的 Wi-Fi 等等。

[image]

返回 - 工具：[image]隐匿点/安全屋周围Wi-Fi入侵检测系统

工具：[image]通过临时Wi-Fi 在设备间离线传输文件

另一个好处是，您可以在用完后直接将其烧掉，并确保它永远消失。（相信诸多 “数字取证” 知识已经吓到很多人了）

不要使用在线的思维导图APP。就用您的纸和笔，尤其是对行动策划来说，这很重要！

如果您是活动家，您有没想过，手绘的动员海报有多大的魅力？它真的很触动人心，比那些色彩斑斓的打印纸要有用得多。

唯一需要注意的是笔迹鉴定。这是法医取证的一部分，除非是激进的直接行动，一般情况下不会遇到。如果您和团队有可能涉及相关风险，可从本站“威胁知识库”进入该主题。

[image]

返回：✍笔迹分析

保持安静

> 说的越少，听到的就越多。

玩过 Kali Linux 的人都会对上面这句话别有感触。俗话说：“愚蠢的人说话，明智的人听”，这不是没道理的。

这种哲学与隐私安全交织在一起，原因很简单：无论您是在现实生活中还是在网上，与人交流的机会越多，邀请他们与您聊天的次数就越多；如果对方刚发了一个大红包，他对您的提问您会不会回答？会不会不假思索全盘托出？…… 然后再后悔吗？

绝不是说您需要怀疑朋友，而是，您和您的朋友通过网络传输的一切都有可能在背后有一大堆人在偷窥，尤其是通过不安全渠道的任何交流，比如微信。

所以您应该时刻意识到这点 —— 并非是您不说政治敏感话题就能“安全”。

沉默是一件美事，在您生活的这个混乱而嘈杂的世界中沉默值得珍惜。通过聆听，与那些滔滔不绝的人相比，您将学到更多。

请注意：这里指的沉默并不意味着完全一言不发，而是说，您需要提醒自己所说的每一个字是否对恶意者有利。

再一次：少即是多。

上传任何东西之前请三思

国家安全局和中央情报局前负责人、臭名昭著的 Michael Hayden 将军有一句名言：“我们基于元数据杀人。”

如果您对最小化和删除元数据的重要性有存有疑问，请记得这句话。

□

延伸：https://web.archive.org/web/20190909083546/https://www.iyouport.org/%E7%96%91%E4%BC%BC%E4%B8%AD%E5%9B%BD%E9%AA%87%E5%AE%A2%E9%92%88%E5%AF%B910%E4%B8%AA%E7%94%B5%E8%AF%9D%E8%BF%90%E8%90%A5%E5%95%86%E7%AA%83%E5%8F%96%E5%85%83%E6%95%B0%E6%8D%AE/

延伸：https://iyouport.substack.com/p/as6-?utm_source=publication-search

[image]

从本站"工具"专题中搜索"元数据"，以查找可能适合您的工具。

您永远不可能知道自己的元数据最终落在什么人手里；更无法预测那些家伙会怎么使用这些东西来对付您。您能做的唯一的事就是，尽可能不要把这些东西放在网上。

您是否仍然认为将所有个人照片上传到 Instagram 和 Facebook 等社交媒体网站、甚至该死的 "云端"，是无害的？那再想想。

可能您的所谓 "好友" 看不到元数据，但是，Facebook、Google、腾讯、百度等等所有这些监视资本家都看得见，而且他们会把这些致命的东西收集起来，给政府间谍，或转卖。他们就是这么发家的。

延伸：https://iyouport.substack.com/p/44a?utm_source=publication-search

任何公司了解您越多，您就越危险；不论他们承诺什么，都不值得您冒险。那是那句话：尽可能缩小被了解的范围，尽可能使用假身份。尽全力保护自己。

[image] 上面大图。

BlackArch Linux

BlackArch Linux是一份基于 Arch 的 Linux 发行版。该发行版被设计用于系统渗透测试及安全研究。

BlackArch 提供一张自启动运行DVD镜像，其中包含有多个轻量级窗口管理器和一千多种用于渗透测试和计算机取证分析的专用工具。

该系统即可以直接从镜像启动，也可以安装在硬盘、U盘或虚拟机上。

众所周知 Linux 是黑客的游乐场，这在很大程度上是由于它是一个免费的开源软件（OSS）操作系统，它提供了比专有OS更高程度的可定制功能。

Linux 发行了太多不同的变体；其中 Kali Linux 也许是最以黑客为主题的Linux发行版，但是鲜为人知的替代方法是 Black Arch Linux。

Black Arch Linux 是一种独特的操作系统（OS）构建，它拥有您想要的几乎所有工具。它是为渗透测试人员设计的这是事实，但是。并不意味着您不能使用它。

大多数普通用户可能不会使用许多这类软件工具，因为使用它们通常需要对计算机和安全工具有深入的了解，但是，其中许多带有图形用户界面（GUI）的工具值得您探索，例如密码破解和恢复被删除文件的工具。

如果您想尝试使用黑客工具，请在家中设置虚拟培训环境。

实现在线虚拟匿名的一种方法是连接到Tor 或 Invisible Internet Project（I2P），I2P是可伸缩性强的具有自我组织与恢复能力的包切换匿名网络；开源软件虚拟化x86引擎，例如可在 Windows、Linux、MacOS 和 Solaris 上运行的 VirtualBox。

您需要首先下载 VirtualBox 并将其安装在计算机上。方法在这里。然后在VirtualBox 内下载并安装 Black Arch Linux 映像（.iso）。

确保已激活VPN，打开 VirtualBox Black Arch Linux 虚拟OS，然后从这里连接到 Tor、I2P 或 Freenet 进行浏览。

就是这样。也许很多人会感觉有点“极端”？但这就是匿名上网的方法，敬业的隐私发烧友和任何尊重人权的公民都肯定会竭尽全力实现

和维护隐私。

应该注意的是：即使使用这种方法进行匿名浏览，警察和间谍仍然有可能将IP地址反向追溯到您的VPN提供商，然后由于 Tor 和互联网中的漏洞，您的VPN提供商可能会被传唤，以索取您的真实IP地址。

当然，如果愿意，您也可以执行相同的技术，在 VMware 上安装 Kali 或 Ubuntu Linux，但是出于本文的目的，我想展示 VirtualBox 和 Black Arch Linux。

认真的 VMware 用户都会告诉您，为 VMware 支付年度订购费用是值得的，而且免费的 VirtualBox 太笨拙了，但是，如果您很节俭，那就肯定会为这一成本犹豫一下。

如果您是重要的公民行动组织的安全部队负责人，我认为您值得花这笔钱。

[image]

黑暗艺术 L33t

被视为黑客术语的 “L33t” （elite精简）需要大量的实践和经验，它也是一种虚拟匿名和不可追踪性的黑暗艺术。

其实并不复杂，它有点像中国网络为了逃避监视而故意编辑的 “敏感词”。通常是把拉丁字母转变成数字或是特殊符号，例如E写成3、A写成@等。或是将单词写成同音的字母或数字，比如 to 写成2、for 写成4等等。

也就是在原文中 “加密”。

拥有 L33t 熟练能力的人可以被认为已经掌握了专门的技艺，一般来说，掌握一门技艺需要大约10,000个小时的经验。

当然，如果加上信息系统安全技术的微妙复杂性，10,000个小时的时间可能还不够。但是，勤动手的习惯绝对能让您更快速进步。

最后，请允许我重复一句：本系列内容并不是为高深的安全领域专家撰写的，他们对这些东西已经非常熟练；我们为的是那些还蒙在鼓里的普通人，通过用最简单的语言描述您的境遇，帮助您了解为什么这些知识都是必要的。

纽约时报的文章中写道，如今“抗议已经变成了极客的特权，而隐私人权难道不应该是普世的吗？”很不幸的确如此 —— 如果您没有足够的自我保护能力，不用说抗议，简单的表达自己的意见都将变得极为艰难。

不是说沉重的猫鼠游戏很好玩，但是必须说，除非我们首先能在这种极端的反乌托邦世界中活下去，否则我们中将没有任何人能再站起来抵抗以终结这个噩梦。

[image]
[image]

大保健应该成为习惯：变得难以被追踪的简单方法S03E06

[image]	关键词	对抗性思考方式 开源情报 数据最小化 社交工程攻击 移动设备 网络攻击 自检
[image]	关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image]	创建时间	2025年4月24日
[image]	**Description**	教材

你的数据就是你的身体＋你的灵魂＋你的人格＋你的财产 ……＋你的一切。

- Table of Contents

  在数据泄露时代维护自己
  社交媒体
  不要让不相关的人了解您太多
  DNA检测
  特色隐私策略，技术和程序
  1、Freenet
  2、I2P
  您的手机
  低技术安全措施：规避和匿名提示
  无人能对攻击免疫
  A：学会跟进
  B：主动使用并鼓励其他人使用端到端加密
  C：不要随便把什么东西插在自己的电子设备上

> 在大规模战略中，当敌人开始崩溃时，您必须在不放过任何机会的情况下追捕他们。如果您没有利用敌人的崩溃，他们可能会迅速康复 —— Miyamoto Musashi

[image]

在数据泄露时代维护自己

在数据泄露时代，我们如何保护自己的个人身份信息（PII）？

为了在似乎每周都有新数据泄露的情况下保持低调，您必须加倍谨慎，尽可能不要将个人信息放在网上。做到这一点的方法是尽可能地在线使用有关您自己的虚假信息 —— 袜子木偶、分身。更多具体做法建议参见本站的“操作安全性”专题。

为什么要使用您的真实姓名、家庭住址和电话号码呢？您知道恶意者可以用这些信息造成多么大的损失吗？很多，完全可以超乎您的想象。

这个世界是一个巨大的舞台，对于那些有足够感知力的人来说，到处都是数字面包屑证据、到处都是微妙的线索、随之而来的是数字足迹。

许多不同类型的人出于多种不同目的使用开源情报工具、方法和技术。有些是网络威胁猎人，有些是罪犯分子，有些将其用于数字取证目的，其他人可能只是想追踪过去的敌人，或用来确定有多少关于自己的个人信息在线 —— 用敌人的眼睛看自己。

我们提供开源情报技术为的正是最后一种目的。

开源情报的的光圈可以根据您的需求任意扩大或缩小。有时搜索范围很广且很深，而其他时候搜索范围又很窄也很浅。

开源情报就是要知道要为特定任务使用哪些工具，这些工具将产生最佳结果，或者要使用哪些工具的最佳组合。毕竟，您可能不会使用高射炮打鸟。开源情报也一样，根据您想要定位的信息，某些工具会比其他工具更好。

开源情报经历了一波高潮，导致大量新软件工具和技术涌现，几乎任何人都可以使用它来收集关于另一个人或组织的“情报”。

有很多软件工具和资源可用于此类调查活动，但是，某些最好的开源情报工具并不是完全设计为工具的 —— 社交媒体本身就可以是最出色的开源情报工具之一。

[image]

社交媒体

如果您重视数字隐私，并且使用 Linkedin 之类的社交媒体网站与上班族联系，那么您面临的侵犯隐私权的可能性比您想象的要大得多。

在 Linkedin 上，除非您正在积极发布有关您自己的虚假信息以摆脱追踪者的困扰，否则，任何人都可以通过您向雇主转发的照片、帖子或资料来查找您的私密信息并可能对您发起攻击，以试图使您被解雇或至少受到谴责。

您为什么要给一个您甚至都不知道是谁的人如此严重的机会？

根据您的个性，与社交媒体上的某人进行火拼可能只是时间问题。您可能是最好、最可爱的人，但是，如果某人不喜欢您写的或发布的内容，那么对您发起战争就是他们的首选项。在这个政治极化的时代，类似 Swatting 攻击这样的事件可能更加频繁出现。

当事情趋向于升级时，您认为那些讨厌您的人会转向什么呢？毫无疑问。

延伸：https://iyouport.substack.com/p/1a0?utm_source=publication-search

坦白说，您无需花大量的网络经验就可以了解开源情报的信息收集工具和技术。换句话说，您不必成为开源情报界专家就可以在短期内让某个人再也爬不起来。所以，您觉得其他人不会这样做吗？

易于追踪就是这个互联网的工作方式，如果您必须使用它，请在这里至少以一个完全不同的身份存在。

[image]

不要让不相关的人了解您太多

在将照片上传到任何网站之前，您是否想过要从照片中删除地理标记元数据？如果没有，您将很容易被这种方式所追踪。

照片元数据被称为EXIF数据，有多种工具可用，任何有经验的人都可以使用这些工具从在线发布的照片中提取EXIF数据。🔙返回本站“工具”专题搜索“元数据”以找到可能适合您的工具。

因此，在任何一种拍照上传之前都请三思！是任何。并不是说您在特殊位置打码就可以了。您永远也不会知道谁潜伏在阴影中。顺便说一些异议人士喜欢在线晒聚会的合影照片，情感需求可以理解，但在大数据加所谓的网格管理的社会控制模式下这类信息可能对涉及其中的每个人都不利。激进派反叛前线尤其应该注意类似问题。

[image] 2012 South African safari tour bus sign, this is not a new phenomenon; credit: Exposing The Invisible

即使一个网站宣传他们会自动删除**EXIF**数据，也请不要轻信，监视资本家从来不会在关于您的利益方面说实话。其逻辑就如中国的“密码法”，只能防隔壁老王，但对警察完全透明，它只能顶个球。

首先考虑一下为什么要在线共享您的个人信息的根本原因。

共享的渴望是否真的源于您内心深处的欲求，还是根本性的空虚、渴望被接受、被大众欢迎或被喜欢？我向您保证，社交媒体不是您的朋友。

[image] 上图中那本书在这里下载：https://t.me/iyouport/6823

回顾一下您使用的所有社交媒体的时间轴，删除任何可能对您不利的内容。在您开始有风险的行动之前，大清洗至关重要。

您永远不会知道谁在收集有关您的信息，更不用说他们会拿来干什么了。因此，您必须采取预防措施，不能等到为时已晚。

如果您不希望完全删除，也确实可以保留一些内容在互联网上，但建议采取以下步骤以减轻伤害。

[image]

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

不论如何，少即是多。请记住，在线发布的内容很有可能将永远保持在线状态。无论在什么地方，它都已存档，或者有人将副本保存到他们自己的硬盘里，进行了截图。

这里说的“删除”只是意味着不大容易找到，但是它们依旧有可能存在。所以最根本性的措施就是，立刻，马上，从现在开始上传任何东西之前都要努力思考其危害性。尤其是如果您的行动/行为涉及到一群人的安全时。

[image]

返回：[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗

返回：[image]社交媒体上的行动主义安全性:框架手册

操作安全永远是第一位，而不是哪个软件；如果您没能注意细节问题，就算最好的防御软件可能也无法保护您。

[image]

返回：[image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

一个宗旨在所有情况下适用：任何他人/公司对您的了解越少，您就越安全。

DNA检测

高风险用户请从“威胁知识库”进入该主题。

[image]

返回：DNA

将您的DNA添加到国家DNA数据库的方式有很多种 —— 这在任何国家都一样，尤其是美国、中国、俄罗斯、印度等有能力这样做的国家，您能做的只有：尽可能避免任何理由的“自愿”DNA测试。

如果您曾经自愿付款提交 DNA，以供 Google 支持的 “23andMe” 或 “Ancestry.com” 之类的公司进行检查，很不幸您已经暴露了。这些寡头公司一直在以世界上所有令人作呕的形式与当权者合作，在这里看到悲惨的教训。

并且，您难道不认为健康保险提供商正在争先恐后地采取可以购买或获得这种遗传信息的任何方式吗？永远不要怀疑那些人的卑劣，他们没有底线。

人寿保险提供商呢？也一样。尽管您为保险付费，但他们比任何人都更希望获得您的遗传信息。

您已经看到了太多的案例，警察用人们自愿提供给祖先检测游戏网站的数据 “解决了” 积压十几年的案子。不要忘了，警察有权获得这些数据 —— 在任何国家都有权。

特色隐私策略，技术和程序

1、Freenet

每当人们想到匿名浏览（尤其是对于暗网）时，就会想到 Tor。但是，还有其他选择，例如 I2P 和 Freenet Project。

[image]

Freenet 是一种免费软件，可让您匿名共享文件、浏览和发布 “freesites”（只能通过 Freenet 访问的网站），以及在论坛上聊天，而不必担心审查。

Freenet 节点之间的通信经过加密，并通过其他节点进行路由，这使得监视者很难确定是谁在请求信息及其内容是什么。

文件会根据其受欢迎程度自动保留或删除，而最不受欢迎的文件将被丢弃，以便为更新或更受欢迎的内容让路。

文件是加密的，通常难以追踪；聊天论坛，网站和搜索功能均基于此分布式数据存储构建。

请注意：即使加密并且仅临时存储在计算机硬盘上，它仍然可以导致严重后果；您如何向政府间谍解释，在您家门口搜出的所谓的非法内容不是您的？

您是否仍然天真地认为检察官或法官会关心 Freenet 分布式数据共享功能的微妙错综复杂性？您是否不同意 Freenet 的使用条款并自行承担下载软件的风险？需要先想清楚这个问题。

2、I2P

[image]

I2P 与 Tor 十分相似，您可将其视为“匿名覆盖网络—网络中的网络”。它旨在保护通信不受诸如ISP之类的第三方进行的窥探和监视。

I2P 被许多关心隐私的人使用：活动家、被压迫的人、新闻工作者、透明度革命英雄、以及想要人权的普通人。

任何网络都不能 “绝对匿名”。I2P 的持续目标是使攻击越来越难以进行。随着网络规模的扩大以及正在进行的学术审查，其匿名性将越来越强。

I2P可在台式机，嵌入式系统（如 Raspberry Pi）和 Android 手机上使用。

如果您不喜欢**Tor**，可以考虑尝试使用**I2P**。

您的手机

超过一半的热点数据隐私问题都来自手机服务提供商；请注意，他们会将您手机的地理位置数据出售给付得起钱的任何人。再一次，在绝大多数国家都是如此。

不幸的是，只要您拥有智能手机，那么您几乎无法采取任何措施来防止这种情况，除非每天连续采取严厉措施。

“严厉措施” 是指，不使用手机时将SIM卡和电池全抠出来。或者随时放在法拉第袋中。（因为如今大多数手机都无法抠出电池）。

□

延伸：https://iyouport.substack.com/p/-snowden?utm_source=publication-search

[image]

返回：[image]你的手机如何背叛了民主？

返回：📱警察如何利用抗议者的手机追踪每个人

返回：[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

低技术安全措施：规避和匿名提示

电子邮件地址的危险程度在某些情况下不亚于手机。您可以在下面回顾一些旧的示例：

□

延伸：https://web.archive.org/web/20200211091358/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E4%BE%A6%E6%9F%A5%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6%E5%92%8C%E7%94%B5%E8%AF%9D%E5%8F%B7%E7%A0%81%EF%BC%9F%E5%BC%80%E6%BA%90%E6%83%85%E6%8A%A5%E8%B0%83%E6%9F%A5%E5%B7%A5%E5%85%B7/

延伸：https://web.archive.org/web/20200306142822/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E4%BB%85%E4%BB%85%E9%80%9A%E8%BF

%87%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB
%B6%E6%8C%96%E5%88%B0%E4%BD%A0%E7%9A
%84%E7%94%B5%E8%AF%9D%E5%8F%B7%E7%A0%81%EF
%BC%9A%E4%B8%80%E7%A7%8D%E6%96%B0/

延伸：https://web.archive.org/web/20200529230112/https://www.iyouport.org/12%E4%B8%AA%E5%BC%80%E6%BA%90%E6%83%85%E6%8A%A5%E8%B5%84%E6%BA%90%EF%BC%9A%E6%8C%96%E6%8E%98%E7%94%B5%E5%AD%90%E9%82%AE%E4%BB%B6%E8%83%8C%E5%90%8E%E7%9A%84%E7%A7%98%E5%AF%86/

所以，您应该致力于使用那些假的一次性电子邮件服务。 在本站“工具”专题中搜索“电邮”，以找到可能适合您的安全电邮解决方案。

尤其是，比如，Netflix 或 Hulu 之类的服务提供免费的限时试用期时，您都可以使用伪造的电子邮件地址获取他们的免费，而不是让他们拿走您的真实电邮地址。所有邀请您注册的新闻平台也一样。

尽可能不注册才是首选。

现在几乎每个网站都要求您创建一个帐户来访问其内容，这很讨厌；所以，您真的值得预备一些一次性的假的电邮地址。

[image]

很多网站要求您提供名字和电子邮件地址。要知道，没人强制要求您提供完全真实的，所以，为什么要给他们真的呢？

[image]

无人能对攻击免疫

良好的生活习惯可以降低感染流行病的风险；这在互联网上也一样，良好的行为习惯能帮助您避免很多常见的攻击。

请记住，没有人能对网络攻击完全免疫，这里没有100%的安全，但安全是一个相对的概念，您只需要做到让自己比其他很多人都更安全，就可以了。

以下几个方法应该成为您的日常习惯。

A：学会跟进

识别网络攻击已经变得越来越困难。带有恶意链接的消息并不总是来自陌生人的。它们可能看起来就像是例行交流，或者似乎起源于您认识或与之合作的人。

攻击者使用的是人类微妙的但根深蒂固的认知偏见 —— 人性漏洞。在本站"心理安全"专题中了解人类固有的弱点，以及防御方法。

还记得这个案例吗？—— 攻击者伪装成国际大牌媒体记者和著名人权组织工作人员，通过加密通讯攻击敏感人士，这可能是建制派异议人士最容易遇到的攻击方式了。□延伸：https://web.archive.org/web/20220129220433/https://www.iyouport.org/%E8%AD%A6%E5%91%8A%EF%BC%9Awhatsapp%E6%96%87%E6%9C%AC%E6%B5%81%E4%B8%AD%E7%9A%84%E6%81%B6%E6%84%8F%E9%93%BE%E6%8E%A5/

值得庆幸的是，您可以使用一种简单的低技术方法来阻止这些攻击：在信任之前先跟进。

具体说就是：如果信息显示它来自您认识的人，去给那个人打个电话，或直接走到他/她面前，问一句："这个是你发给我的吗？"

如果是来自您不认识的人，一概不接受就行了。

也是为什么我们说，您和您的队友之间应该有多种不同的联系方式，包括不同的通讯平台、电话、只有你们双方知道的会面地点和暗号等等。攻击者可能霸占其中一个甚至两个，但很难霸占全部。

如果消息是真实的，那么请过几分钟再进行仔细检查，以确保没有任何危害。

如果不是这样，您应该立刻发出警报：您的熟人已经被入侵，以提醒相关的其他人小心。

B：主动使用并鼓励其他人使用端到端加密

仅仅您一个人使用安全通信是没用的，您应该鼓励您的朋友、同事、亲属都切换到安全IMs。

没有人能独自一个人做到安全，要想保护每个人的人权和安全，我们就需要联合。

这并不意味着您必须完全停止使用其他通信方法，而是将其视为次级选项，或者隔离它们。

[image]

在本站“工具”专题中搜索“Ms”，以查找可能适合您的安全通信工具。

强调：如果是看起来“很重要”的请求或链接，通过被定位为“不重要”的渠道出现在您面前，您应该立刻亮起红灯。

C：不要随便把什么东西插在自己的电子设备上

如果您在人行道的垃圾箱里捡到一个牙刷，您会把它塞进自己嘴里吗？肯定不会对吧。USB设备也是同样的道理。

也许您捡到一个拇指驱动器时会反思一下要不要插进自己的设备，但是，绝大多数人仍然不会怀疑公用的移动设备充电器，和路边小摊卖的**USB**电缆，这是很奇怪的事。

与电子邮件和一些文件共享服务会在文件到达计算机之前对其进行扫描和过滤不同，通过USB插入是直接的且不受保护的。

建立此连接后，用户无需执行任何其他操作即可发生许多可能的灾难。

通过USB连接，恶意软件和勒索软件等问题很容易感染您的设备。

无需宣誓USB连接的便利性，也不必完全避免使用这些设备。但您在任何一次插入之前都应该三思。如果要插入计算机，请确保格外小心。

请直接从制造商或有信誉的公司或具有供应链控制权的经销商处购买USB电缆，而不是街边小店和淘宝。充电时应该使用带有USB端口的壁式充电器。

很有必要养成健康的生活习惯，这是防卫的最佳姿势 —— 将一些认真的网络安全实践纳入您的新10年决议中吧，立即开始实施它们。

[image]
[image]

在雷达下低飞：变得难以被追踪的简单方法 S03E07

[image] 关键词	元数据 分身 加密 合理推诿 隐写术
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月26日
[image] **Description**	教材

有点技术含量，但并非旁门左道。

- Table of Contents

  使用隐写术进行巧妙的欺骗
  创建隐藏在文件中的虚拟加密磁盘
  删除元数据
  监视资本家是隐私权的公敌
  假设一个新的数字身份

[image]

欢迎来到第7集。本集中将要介绍的技术可能要比普通人设想的程度稍高一点点，但绝非偏激，如果您是政治反对派、人权捍卫者、有明确的对手/仇家、希望自己在当下这个世界生活得更加安全自由，那么这些方法您一定要实施。

这个社会中有些人很傻，他们会对那些致力于让自己变得“难以被追踪”的人污名化，站在当权者的立场上说话；尤其是互联网，它鼓励

每个人都成为社交蝴蝶，大胆宣传自己当天的饮食或穿着、甚至每时每刻的想法。那只是为了监视资本家赚钱而已，以您的人权为代价。

不要上当。真的，好人不会那么在乎您的私生活，而您晒的任何东西只能让坏人欣喜若狂。

变得难以被追踪并不是反社会或隐居，这是关于安全和人权的必要措施。

有些人出于绝对必要而努力变得难以被追踪，比如记者、活动家、人权捍卫者、异议人士等等，对他们而言，自我保护已经成为一种生活方式。他们通常非常警惕，几乎在任何时候都不会提供太多个人信息。

对于另一些人而言，掌握一些难以被追踪的技巧就如家里备用的防水胶、电池或阿司匹林，您不知道什么时候就要用到的东西。

我们不是也不应该成为社会价值观的俘虏。这就是在不自由社会中为自己创建一片自由的生活能力。

使用隐写术进行巧妙的欺骗

我们已经多次介绍过隐写术。它有很长久的历史，如今只是在数字技术方面的体现而已。

数字隐写术通常被错误地归类为加密形式，其实它俩截然不同。

的确，许多数字隐写术应用在嵌入过程中都提供了对机密文件进行加密的附加功能，因此，即使你的对手发现了隐藏的东西，在没有相应密码或密码短语的情况下，他们也无法读取机密数据。

隐写术比普通的加密更好在于，它从第一步就能欺骗你的对手，令对

方难以注意到有东西藏在那里。

比如免费的电子邮件服务通常不提供端到端加密或公钥基础结构（PKI），您的私人电子邮件和相关附件可能会在其通过网络传输到目标IP地址的过程中被读取。这些免费电子邮件服务最多可以提供加密的电子邮件收件箱和标准的传输层安全性（TLS）加密。

您可以将浏览器扩展添加到 Chrome、Firefox 和其他浏览器中，提供使用PGP加密电子邮件的功能。加密很好，但它不是看起来那么保密。

依旧可以截取加密的数据包，并通过检查包头来确定发送者和目的地IP地址。使用VPN可以解决这个问题，但并不是完美的，因为VPN提供商仍然知道您的真实IP地址，并且该信息可以由政府和执法部门获取。还有些不可靠的VPN服务提供商会将您的私人浏览数据出售给第三方。

这种情况下隐写术就是最好的东西。监视者看到的是一张猫咪照片和一切不起眼的闲聊，他们很可能不会怀疑“里面”有什么东西。

假设您要发送纯文本（未加密的）电子邮件，并带有隐秘文件附件，这时候您可以搞一些不起眼的文本，例如“嘿哥们，要不要一起吃个饭呢，看看我新买的这辆车怎么样？”。

而监视者看到的只是一堆无聊的闲侃和一张普通的照片。

而真实的文件在照片中加密隐藏，只有使用正确的钥匙（密码/短语）才能打开该文件。

数字隐写术应用程序可以将内容嵌入到几乎现有的任何类型的文件格式中（音频、文本，视频、图像、**VoIP**等）。

[image]

返回：在本站“工具”专题中搜索“隐写”，以查找可能适合您需求的隐写工具。

[image] How digital steganography works; studentweb.niu.edu

就算您不做任何政治敏感的工作，甚至对政治一无所知 …… 您有异地恋吗？您的伴侣正在出远门吗？也许你们之间会有一些希望私密的信息传输。只要双方都同意并具有法定年龄，这不是犯罪。但是，一旦拍摄了那些类型的照片或视频，就很有可能被以某种方式对您不利（例如 报仇色情或勒索），或者将其泄露出去。

安全的思考方式就是尽可能想到所有可能的威胁，并尽可能减轻风险。如果您将这种类型的资料存储在连接互联网的家用计算机或智能手机上，就有可能被盗和被泄漏。

对于您用来制作上述材料的任何摄像机或视频记录设备，都是如此。普通的数字取证工具就可以轻松定位和恢复已删除的文件。。

[image]

激进派行动者请从本站的“威胁知识库”中“数字取证”专题进入相关内容。

您可能还需要隐藏财务信息或密码列表。您也可以使用这种方法，把他们放入只有您一个人知道的极为普通的媒介里面。

互联网上有超过1200种不同的数字隐写应用程序可用。并非所有这些都是一样的，某些应用程序比其他的更成熟，也就是说代码编写得更好。

一些应用程序仅适用于音频、视频、文本或图像文件，而其他应用程序更强大，可以执行更多类型的数字隐写。

您已经熟悉 Mr.Robot 了？Elliot 使用 DeepSound 数字隐写应用程序将数据隐藏在音乐专辑中。为了执行音频或视频文件隐写，载体文件的大小需要大得多，以便能够嵌入隐藏的数据而不会引起音频/视频

文件的明显“失真”。这称为峰值信噪比（PSNR），越低越容易避免被检测到。

这些数字隐写术应用程序中的许多都具有将强大的加密和压缩算法相结合的功能，以将私密文件隐藏在其他文件（称为载体文件）中。接收者在接收之前需要知道解密密钥。

例如，Deepsound 为隐藏的文件提供 AES 256位加密，这是强大的加密，至少在量子计算成为真正的威胁之前。

[image]

创建隐藏在文件中的虚拟加密磁盘

您现在肯定已经知道在所有计算机和电子设备上实施全盘加密的重要性。例如您买了一个手机，您已经知道该制造商在手机上的全盘加密技术是一流的，但是，他们和政府间谍合作 …… 于是该公司的保护技术基本形同虚设。

如果政府间谍有破解 iPhone 加密的方法，那么您就能知道警察和其他政府机构都有访问这些设备的方法，包括外国政府以及网络罪犯威胁者。

我们在本系列第一集中提到过 VeraCrypt，这是法国提供的免费加密应用程序，它允许用户在文件中创建虚拟加密磁盘并将其作为磁盘安装。

VeraCrypt 增强了用于系统和分区加密的算法的安全性，使其免受暴力破解攻击。

VeraCrypt 还解决了 TrueCrypt 中发现的许多漏洞和安全问题，在文件中创建虚拟加密磁盘并将其作为实际磁盘安装，加密整个分区或存储设备，如 USB 闪存驱动器或硬盘驱动器，加密安装 Windows 的分区或驱动器（预启动身份验证）。

加密是自动的、实时的、和透明的，并行化和流水线操作允许读取和写入数据，就像驱动器未加密一样快。

加密可以在现代处理器上进行硬件加速，如果对手强迫您泄露密码，则可以提供合理的推诿：隐藏卷和隐藏的操作系统。

VeraCrypt 是一个用于建立和维护动态加密卷（数据存储设备）的软件，即时加密意味着数据在保存之前就会自动加密，并在加载后立即解密，无需任何用户干预。

整个文件系统被加密（例如，文件名、文件夹名、每个文件的内容、空闲空间、元数据等）。

可以将文件复制到已安装的 VeraCrypt 卷中，也可以将其复制到任何普通磁盘上（例如，通过简单的拖放操作）；在从加密的 VeraCrypt 卷读取或复制文件时，文件会在运行中（在内存/RAM 中）自动解密。

同样，正在写入或复制到 VeraCrypt 卷的文件会在 RAM 中自动加密（在它们写入磁盘之前）。

请注意，这并不意味着要加密/解密的整个文件必须先存储在RAM中才能加密/解密。VeraCrypt 没有额外的内存要求。

假设有一个 .avi 视频文件存储在 VeraCrypt 卷上（因此，视频文件是完全加密的），用户提供正确的密码（和/或密钥）并安装（打开）VeraCrypt 卷。

双击视频文件的图标时，操作系统启动与文件类型相关联的应用程序 - 通常是媒体播放器。然后，媒体播放器开始将视频文件的一小部分初始部分从 VeraCrypt 加密卷加载到RAM（存储器）以便播放。在加载该部分时，VeraCrypt 会自动解密它（在RAM中）。然后，媒体播放器播放视频的解密部分（存储在 RAM 中）。

在播放此部分时，媒体播放器开始将另一小部分视频文件从 VeraCrypt 加密卷加载到 RAM，然后重复该过程。此过程称为动态加密/解密，适用于所有文件类型。

例如，在过境时，这可能会很有用，因为您会被搜查电子设备；同样，在国内，如果您认为自己有被警察搜查电子设备的风险，它也会有用。

如果您由于某种原因而被拘留，并且政府机构威胁您要求密码解锁您的加密驱动器。您就可以假装不情愿地给他们密码，他们只能看到被放置在外面的相对无害的东西。

[image]

删除元数据

这不是第一次提醒了。

麻省理工学院开发的一个名叫 Immersion 的程序，仅需使用元数据就可以绘制出您的邮箱中所有电子邮件的发件人和收件人之间的可视化关系图。

谁对您（目标人）最重要，一目了然。程序甚至包含一个滑块式的时间标度，可以让您看到您认识的人对您的重要性随时间推移发生的起起伏伏。

尽管您可能认为您了解自己的关系，但用图形化的方式表达出来，也许会给您带来清醒的认识。

您可能没意识到自己给不认识或了解不多的人发了如此多的电子邮件，却很少给非常熟悉的人发邮件。

使用 Immersion工具，您可以选择是否上传数据，而且在图形绘制出

来后，也可以删除这些信息。

在将任何图像上传到网站或通过电子邮件发送给其他人之前，建议您首先筛查删除元数据。您需要担心的不仅仅上政府间谍，还有各种恶意者，他们会通过元数据对您在现实中进行跟踪伤害。您不值得冒这种风险。

监视资本家是隐私权的公敌

谷歌、Facebook 等监视资本家已经被国际特赦组织谴责为人权侵犯者，虽然有点晚，但依旧很重要。Nithin Coca 写了一篇漂亮的文章，讲述了他为什么完全放弃使用 Google，以及为什么您也应该这样做。

如何您想要隐私人权和人身安全，谷歌不是您的朋友，Facebook、Twitte、Instagram 等等都不是您的朋友，他们赚到的钱都是通过出卖你得来的。每个人都应该知道这一点。

[image]

返回：[image]消除对 Google Web 服务依赖的轻量级方法

返回：[image]谷歌 “查找我的设备”的安全开源替代

返回：[image]Google Drive 的开源替代产品

返回：[image]隐私自助：流行产品的开源替代品目录

假设一个新的数字身份

如果您感到不知所措，并且需要为数字生活排毒，那么从现在开始控

制自己的数字生活还来得及，且非常重要；尤其是，您需要开始清理曾经暴露在互联网上的一切 - 那其中包含可能带来危险的东西。

这也许是一项费时的工程，但非常有必要。而且要知道，信息一旦上了互联网，就很难彻底删除，要有这个思想准备。

但残留的越少安全性就越高，于是您依旧值得采取措施。用简单的开源情报工具和方法就可以帮您检查自己的漏洞，抢在包括政府间谍在内的恶意者之前采取行动弥补漏洞。

[image]

返回：[image]如何跨社交媒体平台追踪目标人：对抗性思考方式

[image]

如果您因为上瘾而不能放弃社交媒体帐户活动，也没关系；我们推荐过制作袜子木偶的方法（见下面）。制作并不难，关键在于维护 —— 您始终需要保持这些伪装身份不能以任何方式与您的真实身份相关联。

[image]

高风险用户建议从“威胁知识库”进入该主题 - “分身”。

[image]

返回 - 同主题演示：[image]大清洗 - 扫荡危险区域：完美隐身 S04E07

如果您对此没有信心，也可以通过不定期更改社交媒体个人资料来至少缓解可能的风险 —— 包括用户名、ID、头像、简介、内容偏好等等。

一些黑客会这样做。他们在同一平台上以不同的角色维护多个不同的社交媒体帐户。

某些社交网站可能会限制您更改个人资料的频率，甚至要求您删除旧帐户并以新帐户重新开始。监视资本家试图使您的退出变得尽可能困难，以防止用户放弃其服务，他们只为了保护他们自己的利益。而不是您的。

对于那些拥有大量社交媒体关注者的人可能不希望这样做，担心粉丝找不到。于是您需要权衡，究竟是虚拟的所谓知名度更重要，还是您的真实安全更重要。

如果粉丝经济是您的唯一收入来源，比如您经营网店或者做其他在线生意，那么更建议您尽可能采取上述提到的分身方法，将吸引粉丝的角色和您的真实角色区分开。

比如类似以下这样的服务。

- AccountKiller（https://www.accountkiller.com）提供了有关如何删除大多数热门网站上的帐户或公开个人资料的说明。

- JustDelete Me（http://justdelete.me）是一个直接链接目录，用于从Web服务中删除帐户。

一些公司，例如 Lifelock 和 Experian，正在提供暗网扫描服务，作为身份盗窃监测工具。我们认为您不需要在这种产品上浪费钱。这些扫描的作用不大，而且很可能只在极少数几个非法黑市中寻找。

暗网上有各种类型的隐藏服务和站点，其中一些仅由了解他们的个人与他们选择邀请的受信任人共享。这种几乎无法 “扫描” 出来。

如果您有投资这种东西的钱，还不如投资一些真实的自我保护技术，尤其是从日常操作习惯方面努力，您将看到真实的效果。

可惜的是，对于中国境内的数字用户而言，目前为止还没有简单的快

速清除数据的方法。您只能通过自我人肉查找到曾经使用真实身份注册过的账户，然后手动清理。

总之，要想防御敌人，就需要像敌人一样思考。尽量不要让别人有理由注意到您、甚至追踪到您。在雷达下低飞。

[image]
[image]

到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

[image] 关键词	电话 移动设备 端对端加密
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年4月28日
[image] **Description**	教材

整体解释一下关于窃听的事，尤其是为什么重要场合您不应该使用手机。

- Table of Contents

  手机本质上就是一个追踪设备
  那么要如何避免被追踪呢？
  如果可以渗透进**SS7**，就可以操纵通话
  在移动设备真正普及之前，窃听就已经存在了
  数字电话让监视更简单了
  端到端加密移动**VoIP**

[image]

手机本质上就是一个追踪设备

移动设备使用的蜂窝服务是无线形式的，依赖于蜂窝塔，即基站。为

了保持连接，手机会持续不断地向离自己最近的一个或多个蜂窝塔发送信标信号。

这些塔对于信标信号的应答会被翻译成您手机上“信号格”的数量：一格也没有就表示没信号。

[image]

参加敏感的活动和聚会时最好不要带自己的手机。或者用多层铝箔纸包裹起来。

返回：[image]你的手机如何背叛了民主？

为了以某种方式保护用户的身份，手机的信标使用了所谓的国际移动用户识别码（international mobile subscriber identity，IMSI），这是分配给SIM卡的一个独特数字。

它最初诞生的时候，蜂窝网络还需要知道您什么时候连接到它们的塔上，什么时候在漫游（即使用其他运营商的蜂窝塔）。

IMSI码的第一部分指明了特定的移动网络运营商，其余部分则向该网络运营商标识了您的手机。

全球的警察已经制造出可以伪装成蜂窝基站的设备黄貂鱼，而且使用很多年了。这些设备是为拦截语音和短信而设计的。

[image]

对于高风险用户，请从“ 威胁知识库 ”进入“ 黄貂鱼 ”主题。

在一些国家，维稳部门和间谍机构也会使用其他设备来获取IMSI。

IMSI可以被即时获取，一秒钟都用不了，而且也不会发出预警。

通常镇压当局会在大型集会上、也就是抗议活动现场，使用黄貂鱼，这样就可以让维稳部门在后方识别出谁在现场，尤其是那些不断打电话叫其他人加入的人 —— 作为召集者会最先被捕。

这样的设备也可应用于通勤服务和创建交通报告。在这种情况下，实际账号或IMSI并不重要，重要的是您的手机从一座塔到另一座塔或从一个地理区域到另一个地理区域的速度。

手机接近和远离每一座塔所用的时间可用来确定交通状况：堵塞、缓行或畅通。

只要您的移动设备开机，它就会连接到一些蜂窝塔。离您最近的塔会实际地处理您的电话、短信或互联网通话。

当您移动时，手机会与最近的塔进行回环应答（ping），如果有必要，您的通话也会从一座塔转移到另一座塔，同时还能保持连贯性。

附近的其他塔全都处于待命状态，这样当您从地点A移动到地点B并且进入了信号更好的另一座塔的区域时，信号就会平滑地切换，您应该也不会掉线。

可以这样说：移动设备发出一段特定的序列，这段序列会被多座单独的蜂窝塔记录下来。

所以，任何人只要查阅一座特定塔的日志，就可以看到在其全部区域内任意给定时间所有人的临时移动用户识别码（temporary mobile subscriber identity，TMSI），不管他们是否打过电话。

维稳部门可以、并且也确实会要求蜂窝运营商提供这些信息，包括特定持有人的后端账号身份， 全球都是如此 。

一般来说，如果只查看一座信号塔的日志，其数据可能仅仅表明某个人正在经过，而且他的设备连接到了一座待命的特定信号塔。

如果其间有通话或数据交换，那还会有关于那次通话和持续时间的记录。

然而，来自多座信号塔的日志可被用于精确定位一个用户的地理位置。

大多数移动设备每次会与3座或更多的塔进行回环应答。使用来自这些信号塔的日志，某人可以基于这些回环应答的相对强度，通过三角定位来确定该手机用户的一个相对准确的位置。

延伸：https://iyouport.substack.com/p/1200?utm_source=publication-search

延伸：https://iyouport.substack.com/p/blm1?utm_source=publication-search

所以，准确说，您每天带着到处走动的手机本质上就是一台间谍设备。

[image]

那么要如何避免被追踪呢？

[image]

高风险学习者可从“威胁知识库”进入相关主题 - 自卫措施 - 匿名手机。

与手机运营商签订合约需要姓名住址和身份证号，此外还可能有信用检查，以确保您付得起月租费。

一次性手机看上去是个不错的选择。理论上频繁更换（比如说每月甚

至每周）预付费手机，也许就可以避免留下太多痕迹。

您的 TMSI 会出现在一座信号塔的日志中，然后又会消失。如果您购买手机时也很谨慎，用户账号就不会被追踪到。预付费手机服务仍然有用户账号，所以也会有分配给它的IMSI。

因此，一个人的匿名性取决于他获得一次性手机的方式。在下面看到详细介绍，非常重要！

[image]

假设你已经成功地与一部一次性手机的购买行为断绝了身份关系 ——比如让一位与您完全无关的人使用现金购买了这部手机。那么使用这种用后即抛的手机就不会被追踪了吗？简而言之，不行。

这里就有一个警示故事：

2007年的一个下午，一个价值5亿美元的装满迷幻药的集装箱在澳大利亚墨尔本的一个港口丢失。臭名昭著的毒贩 Pat Barbaro 是这个集装箱的主人。他把手伸向自己的口袋，拿出自己12部手机中的一部，拨打了当地一位记者 Nick McKenzie 的号码。这位记者只知道打电话的人名叫 Stan。Barbaro 随后会使用他的另一部一次性手机给 McKenzie 发短信，试图匿名地从这位调查记者手里获得有关这个丢失的集装箱的信息。正如我们将会看到的那样，这种方法没用。

尽管很多人可能认为一次性手机是真正匿名的，但实际上并非如此。

比如，根据美国的《法律执行通信协助法案》（Communications Assistance for Law Enforcement Act，CALEA），与一次性手机连接的所有IMSI都要上报，就像那些主流运营商的合约用户一样。

换句话说，警察可以根据日志文件找到特定的一次性手机，就像找到注册的合约手机一样简单。

尽管无法通过 IMSI 确定谁拥有这部手机，但也许可以通过使用模式来确认。

澳大利亚没有 CALEA，但执法人员仍然可以使用相当传统的方法密切监视 **Barbaro** 的众多手机。

比如，他们可能会注意到 Barbaro 首先用自己的个人手机打了一个电话，几秒钟后又在同一个基站的同一日志文件中看到来自他的某部一次性手机的电话或短信。

随着时间推移，这些 IMSI 在同一基站同时出现的频次会高于正常水平，这个事实可能就说明了它们属于同一个人。

Barbaro 有很多手机可以随便使用，但问题是，不管他使用哪部手机，不管是个人手机还是一次性手机，只要他待在同一个地方，信号就会到达同一座蜂窝塔。

他的一次性手机总是出现在他注册的手机旁边。而这部注册手机已经在一家运营商那里关联了他的名字，完全可以被追踪，以帮助执法部门确定他的身份。

这为针对他的案件提供了确凿的证据—— 尤其是这种模式也在其他地方重复出现，帮助澳大利亚当局成功认定 Barbaro 组织策划了澳大利亚史上规模最大的迷幻药走私案并将其定罪。

记者 McKenzie 总结说：“自从手机在我的口袋里振动、‘Stan’ 短暂地进入我生活的那天，我就格外清楚人们的通信会如何留下痕迹，不管他们有多谨慎。”

当然，您可以只用一部一次性手机。这就意味着您时不时需要使用预付卡或比特币匿名购买额外的使用时间。您可以在修改了无线网卡的MAC地址后使用一个公开的 Wi-Fi 安全地做到这件事，并且要躲开任何摄像头的视野。

或者雇一个陌生人去店里用现金购买预付费的手机和几张充值卡。这会增加成本，也可能不方便，但您会得到一部匿名的手机。

[image]

如果可以渗透进SS7，就可以操纵通话

延伸：https://iyouport.substack.com/p/-ss7-f2b?utm_source=publication-search

尽管蜂窝技术听起来可能很新潮，但它其实已经有超过40多年的历史了，而且就像铜线电话系统一样，它传承着一些可能危害您的隐私的技术。

每一代手机技术都有新功能，主要目的是更高效地传输更多数据。

20世纪80年代的第一代手机（1G）让人们用上了移动通信技术。这些早期的1G网络和手持设备都是基于模拟技术的，而且它们使用的是现在已经停用的各种移动标准。

1991年，第二代（2G）数字网络推出。2G网络提供了两个标准：全球移动通信系统（GSM）和码分多址（CDMA）。它也推出了短消息服务（SMS）、非结构化补充数据业务（USSD）以及其他今天仍在使用的简单通信协议。

目前已经迈进5G时代。 无论运营商采用了哪一代技术（2G、3G、4G或4G/LTE），其底层都有一个国际性的信号协议，被称为信令系统（signaling system）。

这个信令系统协议及其他事物能帮助你在高速公路上驰骋，并且在从一座信号塔到切换到另一座信号塔时保持移动通话的顺畅连接。

它也可被用于监视。

7号信令系统（signaling system 7，SS7）基本上能够完成路由通话所必需的一切，比如：

- 为通话设置一个新连接；
- 当通话结束时中断连接；
- 正确地为通话计费；
- 管理呼叫转移、主叫方名称及号码显示、三方通话和其他智能网络（IN）服务等额外功能；
- 免费电话和长途电话；
- 无线服务，包括用户身份识别、运营商和移动漫游。

在德国柏林举办的年度计算机黑客大会——混沌通信大会（CCC）上，Sternraute 创始人 Tobias Engel 和安全研究实验室（Security Research Labs）的首席科学家 Karsten Nohl 在演讲中解释道，他们不仅可以定位世界上任何地方的呼叫者，还能窃听这些人的电话交谈。

而且即便无法实时窃听，他们也可以将加密的电话和文本录下来，之后再解密。

在安全领域，您的安全程度取决于您最薄弱的环节。

Engel 和 Nohl 发现，尽管发达国家已经在开发相对安全和隐私的3G、4G网络上投入了数十亿美元，但它们仍然必须使用SS7作为底层协议。

SS7可以处理呼叫建立、计费、路由和信息交换功能的整个过程。这意味着如果你渗透进SS7，您就可以操纵通话。

SS7允许攻击者利用尼日利亚这类国家的小型运营商获取欧洲或美国的电话呼叫。

Engel 说：“这就像是你锁好了房子的前门，后门却大敞四开。”

这两位研究者测试了一种方法，当攻击者使用电话的呼叫转移功能时，SS7会将目标对象拨出的电话转移给自己，之后再通过会议模式（三方通话）将接听者拉进来。

一旦攻击者做好了安排，就可以窃听目标对象在世界任何地方拨出的所有电话。

攻击者可用的另一个策略是，设置无线电天线来收集一个给定区域内的所有蜂窝通话和短信。

对于任何加密的3G通话，攻击者都可以要求SS7提供正确的解密密钥。

> “这全都是自动化的，只需要按一个按钮，这种间谍能力很完美，让我震惊，它可以被用来记录和解密几乎任何网络……任何我们测试过的网络都有效。”

由于所有运营商为了提供服务都必须追踪它们的用户，所以SS7还提供了其他功能，如今仍然可以做到某种程度的远程监视。

[image]

在移动设备真正普及之前，窃听就已经存在了

Anita Busch 的噩梦始于2002年6月20日的那个早上，邻居急促的敲门声惊醒了她。某个人在她的汽车风挡玻璃上留下了一个弹孔，当时她的车停在车道上。不仅如此，汽车的引擎盖上还留下了一朵玫瑰、一条死鱼和一张字条，上面写着一个词：“Stop”。

之后她知道自己的手机被窃听了，但并不是警察干的。 事实上，这个有一个弹孔和一条死鱼的场景是为了让人想起一部糟糕的好莱坞黑帮电影，由此就能理解其背后要表达的意思了。

Busch 是一位经验丰富的记者，她受《洛杉矶时报》的委托，刚刚开始几周的自由撰稿人工作，准备记录有组织犯罪在好莱坞日益增长的影响。

当时她正在调查 Steven Seagal 和他的前商业合作伙伴 Julius R. Nasso —— 调查已经表明，Nasso 正与纽约黑手党密谋向 Seagal 敲诈钱财。

发现她车上的那张字条之后，她又收到了一系列电话。打电话的人显然想告诉她一些关于 Seagal 的信息。再后来，Busch 了解到这个打电话的人受雇于 Anthony Pellicano，他曾经是洛杉矶的一个著名的私家侦探。

在 Busch 的车被人动了手脚之后，FBI 就已经怀疑 Pellicano 有非法窃听、贿赂、身份盗用和妨碍司法公正的行为了。

Busch 的有线电话已经被 Pellicano 窃听。通过窃听 Busch 的电话，Pellicano 知道她当时正在写一篇关于他的客户的新闻报道。放在她车子上的死鱼是想警告她，让她停手。

窃听通常不只与电话有关，一些与窃听相关的法律也覆盖了对电子邮件和即时消息的窃听。

这里的重点是有线电话的传统窃听。

有线电话是您家或公司里面用实际的线缆连接起来的电话，而窃听也真正涉及切入真实的线缆中。

那时候，每家电话公司都有某种实体的开关库，它们可以在此之上执行某种形式的窃听。也就是说，电话公司有一些特殊的装置，而其框架技术可以将这些装置连接到中央办公室中主机上的目标电话号码。另外，还存在一些呼叫这些装置的额外的窃听设备，可用于对目标进行监控。

现在，这种监听方式已经退休了，电话公司全部被要求实施CALEA规定的技术要求。

尽管现在越来越多的人都转向了移动电话，但很多人仍然保留着有线电话，因为他们觉得这些铜线连接的电话很可靠。

其他人也使用被称为基于IP的语音传输技术（Voice over Internet Protocol，简称VoIP），这是一种通过互联网打电话的技术，通常与您家里或办公室里的有线电视或互联网服务绑定在一起。

无论是利用电话公司里的实体开关还是数字开关，警察都有能力窃听通话。

1994年的CALEA要求电信制造商和运营商修改它们的设备，以便执法部门能够窃听其线路。

所以根据CALEA，理论上美国境内所有有线电话的通话都很容易被拦截，而且所有执法部门都需要
Title III 授权令才能读取这些电话。也就是说，普通公民的窃听行为仍然是违法的，而私家侦探 Anthony Pellicano 为了窃视记者和其他人就这么做了。

被他窃听的受害者还包括 Sylvester Stallone、David Carradine和 Kevin Nealon 等好莱坞明星。

Pellicano 窃听别人的目的是试图恐吓证人，使其以特定的方式不做证或做假证。

您可能会问，使用铜线连接的、显然要被窃听的有线电话时，怎样才能隐身？答案是，不能隐身，除非购买专用设备。至于那些真正的偏执狂，可以选择一种能在铜线上加密所有语音通话的有线电话。

这种电话确实能解决私人电话被窃听的问题，但必须要通话双方都使用加密才行；否则可能还是很容易被监控。

对普通人来说，有一些关于电话的基础选择可以让我们避免被窃听。

[image]

数字电话让监视更简单了

数字电话的发展没有让监控行为变得更难，反而使其更简单了。

今天，如果要对一条数字电话线路进行监控，完全可以远程实现。电话交换计算机只是简单地创建了另一个并行的数据流；不需要任何额外的监控设备。这也让人更加难以确定一条给定的线路是否遭到了窃听。

而且在大多数案例中，这样的窃听都是偶然被发现的。

在希腊举办了2004年夏季奥运会之后不久，沃达丰（Vodafone）旗下的 Vodafone-Panafon 的工程师从公司的蜂窝网络中移除了一些流氓软件，这些软件被发现时已经在那里运行了一年多了。

实际上，警察会截取经由任何蜂窝网络发送的全部语音和文本数据，为此他们会使用一种被称为RES的远程控制系统，该系统是模拟信号窃听器的数字等效形式。

当被监视的目标拨打电话时，RES会创建另一个数据流，并将其直接传送给执法人员。

在希腊发现的这些流氓软件进入了沃达丰的RES，也就意味着在正规执法部门之外，还有其他人也一直在窃听经由其蜂窝网络进行的通话；在这个案例中，窃听者感兴趣的是政府官员。

在这届奥运会期间，有的国家（比如美国和俄罗斯）为国家级的通话提供了它们自己的私密通信系统。来自全世界的其他国家首脑和企业高管，使用的则都是已经受损的沃达丰系统。

调查表明，希腊总理及其妻子的通信在奥运会期间受到了监控，雅典市长、希腊欧盟专员、国防部、外交部、商船部和司法部的通信也未能幸免。

另外，反全球化组织、执政的新民主党、希腊海军总参谋部的成员、和平活动人士和美国驻雅典大使馆的一位希腊裔美国员工的电话也遭到了截听。

要不是沃达丰在调查另一起不相关的投诉（短信传送失败的比例高于正常水平）时找来自己的RES系统供应商爱立信（Ericsson），这种间谍活动可能还会持续更长时间。

在执行了问题诊断之后，爱立信告知沃达丰：发现了流氓软件。 不幸的是，十多年过去了，仍然不知道谁是幕后黑手或原因为何。

甚至不知道这种活动有多普遍。

而更糟的是，沃达丰显然没有妥善做好调查工作。

一个表现就是，覆盖该事件的关键日志文件丢失了。而且沃达丰没有在发现这个流氓程序后让其继续运行（这是计算机犯罪调查中的普遍做法），反而唐突地将其移出了它们的系统，这会给作案者提供预警，让他们可以进一步掩盖自己的踪迹。

沃达丰事件是一个让人不安的警示，提醒了要拦截你的手机是多么容易。

但即使您用的是数字电话，也有可以实现隐身的方法。

[image]

端到端加密移动VoIP

除了手机和老式的有线电话，还有第三种电话选择**—— VoIP**。

VoIP适用于任何本身不带电话功能的无线设备（比如苹果的 iPod Touch），比起传统的打电话，这更像是网上冲浪。

有线电话需要铜线；移动电话使用信号塔；而 VoIP 通过互联网传输您的语音—— 不管使用有线还是无线的互联网服务。

VoIP 也适用于移动设备，如笔记本电脑和平板电脑，无论它们是否具有蜂窝服务。

为了省钱，很多家庭和办公室都已经切换到了VoIP系统，这些系统是由新服务提供商和已有的有线电视公司提供的。

为各个家庭传输视频流和高速互联网的同轴电缆也可供VoIP使用。

好消息是VoIP确实会使用加密，尤其是一种被称为“会话描述协议安全描述”（session description protocol security descriptions，简称 SDES）的加密方法。

但也有坏消息，**SDES**并不是很安全。

SDES的部分问题在于其加密密钥不是通过安全的SSL/TLS（一种网络加密协议）分享的。但是，如果供应商不使用SSL/TLS，那密钥就是明文发送的。

它使用了对称加密，而不是非对称加密，这就意味着由发送方生成的密钥必须以某种方式传递给接收方，才能为电话解码。

假设小李想给在外国的小红打电话。小李用SDES加密的VoIP电话为这场通话生成了一个新的密钥。

小李必须以某种方式让小红也得到这个新密钥，这样她的VoIP设备才能解码他的电话呼叫，他们才能进行交谈。

SDES提供的解决方案是，将该密钥发送给小李的运营商，然后传递给小红的运营商，再分享给小红。

您看到哪里有问题了吧？

接收方在另一端解密之前，通话一直保持加密状态。但SDES将来自小李的密钥分享给了小李的运营商，如果小红的运营商和他的不同，那么这场通话从小红的运营商到小红本人的阶段是加密的。

中间的缺口大不大还存在争议。

使用 Skype 和 Google Voice 的情况也与之类似。每当一个电话发起时，就会有新密钥生成，但这些密钥之后就传递给了微软和谷歌。

幸运的是，现在有一些可以端到端加密移动**VoIP**的方法。 来自 Open Whisper Systems 的 **Signal** 是一个免费的开源的手机**VoIP**系统，可为 **iPhone** 和安卓提供真正的端到端加密。

Signal 的主要优势是其密钥管理仅在通话双方之间处理，不会通过任何第三方。也就是说，就像在SDES中一样，每次通话都会生成新的密

钥，但这些密钥的唯一副本存储在用户的设备上。

因为 CALEA 允许读取任何特定电话的记录，那么在这种情况下，执法部门只能看到这家移动运营商的线路上有加密的流量，而无法了解其内容。

而且开发了 Signal 的非营利组织 Open Whisper Systems 也没有这些密钥，所以授权令也无法使用。

这些密钥仅存在于通话两端的设备上。

而且一旦通话终止，这些会话的密钥就会被销毁。

CALEA 目前还没有延展到终端用户或他们的设备上。

但在使用方面有一些注意事项，详见下面。

[image]

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

您可能认为在手机上使用加密会榨干您的电池。加密确实会耗电，但也不会消耗太多。Signal 会推送通知，就像 WhatsApp 和 Telegram 这些应用一样。因此，只有来电呼入时，您才会看到这些通知，而当您接听新来电时，这些通知的耗电量就减少了。

安卓和iOS应用也会使用移动网络必备的音频编解码器和缓冲算法，所以同样在您打电话时，加密本身并不会耗费太多电量。

除了使用端到端加密，Signal 还使用了完全正向保密（perfect forward secrecy，PFS）。

PFS是什么？这种系统为每一次通话都使用了稍有不同的加密密钥，

所以就算真的有人拿到您加密的电话通话及用于解码该通话的密钥，您的其他通话仍然是安全的。

所有PFS密钥都基于单个的原始密钥，重要的是，即使有人拿到了一个密钥，也并不意味着您的潜在敌人能够进一步读取您的通信。

最后必须再次强调：任何一个软件都无法保护您的全部安全！要想尽可能获得真正的安全，您需要安全文化 —— 并保证在您的亲密关系内切实实施它。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

[image]
[image]

8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09

[image] 关键词	加密货币 匿名购买 自检 虚拟机
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年5月1日
[image] **Description**	教材

一个小错误就可能前功尽弃。但是错了不是死刑，您可以再来一次。

- Table of Contents

  第一步：最好能有一台单独的笔记本电脑，便宜点的就行
  第二步：匿名购买一些礼品卡
  第三步：连接**Wi-Fi**时修改你的**MAC**地址
  第四步：匿名创建电子邮件
  第五步：将礼品卡变成比特币并进行清洗
  第六步：如果匿名性受损，那就再匿名一次
  第七步：随机改变您的正常打字节奏
  第八步：时刻保持警惕

[image]

全面的在线安全需要采取哪些步骤？会花多少时间、多少钱？

实际上可以不需要花很多钱，但必需花一些心思。

您首先必须创建一个单独的身份，一个与您本人完全无关的身份。这

就是匿名的含义。您必须严格地将现实和在线匿名身份彻底切分。在下面看到方法：

[image]

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

返回：[image]袜子木偶 - 分身创建的小技巧

最好的是，您应该使用一台单独的设备，也就是说，您的匿名身份完全在这台单独设备上进行，而不是您操作过真身份的设备。但是这可能比较费钱。

不过您至少可以使用虚拟机来分离不同身份。虚拟机是一种软件计算机，它被包含在VMwareFusion 等虚拟机应用中。您可以在虚拟机中加载一个授权的 Windows10 副本，并告诉它您需要多少RAM、多少磁盘空间等。

延伸：https://iyouport.substack.com/p/--62e?utm_source=publication-search

对于监视者来说，这看起来就像您在使用一台 Windows10 电脑，而实际上您用的是Mac。

安全研究人员和开源情报调查人员一直使用虚拟机，可以轻松创建并随时销毁它们。但即便是专业人士也会面临着隐私泄漏的风险。

比如，您可能在您的虚拟机版本的 Windows10 中，而因为某种原因登陆了您自己的电子邮件账户，现在这个虚拟机就与您的真实身份关联起来了。别犯这种错误。

操作安全永远是首要条件，而非哪个软件。

[image]

高风险学习者请进入本站“操作安全性”专题查询您需要的内容。

直接行动者请从本站“ 威胁矩阵 ”进入该主题 分身

第一步：最好能有一台单独的笔记本电脑，便宜点的就行

如上，如果您使用虚拟机，当然可以省钱，但也许不太容易避免那种操作错误的发生。当然，如果您有信心的话，那是另一回事。

其实只需要一台低价位的 Windows 即可，Linux 更好。跳过注册 Windows 账户的步骤，不要将您的电脑和微软之间建立明显的联系。

您应该亲自使用现金购买这台电脑，而不是在网上买，这样才不会被购买行为追踪到您。

您的独立设备中有一个带有独特MAC地址的无线网卡，您不希望任何人利用这台设备追溯到您 —— 您的真实MAC地址可能在某个事件中以某种方式泄漏了。比如，您在一家星巴克打开过笔记本电脑，系统就会自动探测任何以前 “连接过的” 无线网络。

如果这一区域有记录探测请求的监控设备，就可能会导致你的真实MAC地址泄漏。

一个问题是，如果您的网卡的MAC地址和您的笔记本电脑序列号之间存在任何联系，间谍机构就有办法追溯到您的笔记本电脑的购买事件。如果是这样，政府间谍只需要找到购买这台电脑的人是谁，就可以确定您的身份，这并没有那么困难，

所以您应该同时安装 **Tails** 和**Tor**，而不是使用自带的操作系统和浏览器。

不要用您的真实身份登陆任何网站或应用。您已经了解了在互联网上追踪一个人有多容易，所以您知道其中的风险。

实际上，您在家启动匿名笔记本电脑之前，也最好关闭无线路由器。如果您连接到了家庭路由器（假设您的服务提供商拥有并管理着您家里的路由器），那么他们就能得到您的这台电脑的MAC地址。

最好的方法一直都购买您自己能拥有完全控制权的家庭路由器，服务提供商只能看见您的路由器MAC地址，这对您来说风险不大。

您需要的是看起来合理的可否认性。您需要为您的连接设置多层代理，从而让追踪者难以将它们与单个人关联在一起。

永远不要在家里和工作场所直接使用您的匿名电脑，并且保证不要使用它查阅与您本人有关的任何账户，例如 电子邮件、社交网络、甚至包括本地天气。

第二步：匿名购买一些礼品卡

追踪资金流是追踪一个人的最便捷方法，这就是为什么必须抵制在线支付。

但您需要为一些东西付费，所以在将您的匿名笔记本电脑带出去找到一个公开的无线网络之前，第一步是匿名购买一些礼品卡。

因为每家销售礼品卡的店里尤其是柜台处都有监视摄像头，因此您需要格外小心。您可以在街头临时雇佣一个人帮您去买，您自己在安全的距离之外等候。用现金购买。

如果您住在欧盟国家，可以使用 viably.com 匿名购买一张实体信用卡。商家可以将这些卡通过邮局寄送，取货时不需要ID。他们会发送给你一个PIN码，你可以通过输入这个PIN码取走商品 —— 假设储物柜没有摄像头的话。

[image]

第三步：连接Wi-Fi时修改你的MAC地址

所以您可以在哪里使用您的新笔记本电脑和匿名购买的预付费礼品卡呢？

随着更便宜的光存储设备出现，提供免费无线访问的企业可以将监控摄像头录像存储数年之久。政府间谍可以轻松获取这些录像。他们还可以分析在您访问期间的日志 —— 搜索在其无线网络上验证过的与你的MAC地址匹配的地址。

所以，每当您连接到一个免费的无线网络时，修改**MAC**地址很重要。您需要找到一个靠近提供免费无线接入的机构旁边比如一家餐馆，要坐在靠近该服务提供商的墙旁边。可能会感觉网速慢一点，但是会比较安全（至少在追踪者查看周围区域所有监视器之前）。

一旦您在免费无线网络上进行了认证，您的MAC地址就很可能会被记录并保存下来。前中情局局长 Petraeus 的情妇在酒店登记的时间和日期与她的MAC地址在这家酒店网络上出现的时间和日期相匹配，她就是这样被发现的。

您不会希望犯这种错误。所以要记住，每次接入公共Wi-Fi时，都修改您的MAC地址。

永远不要在打开您的匿名笔记本电脑、一次性手机的同一个地方打开您的个人手机或个人笔记本电脑。这种隔离是相当重要的。在之后的某个时间，能将您本人和您的匿名身份关联到一起的任何记录都会让所有操作毁于一旦。

第四步：匿名创建电子邮件

从现在开始，使用Tor浏览器来创建和访问所有网站账户。

第一步就是，设置几个匿名的电子邮件账户。

这是 Ross Ulbricht 疏忽大意没有做到的事。他在暗网上进行 “丝绸之路” 业务时不止一次使用了他的个人电子邮件账户。“恐怖海盗罗伯茨” 和 Ross Ulbricht 两个身份之间无意中出现的这些交集帮助政府间谍确认了它们之间的关系。

[image]

在本站“工具”专题中搜索“电邮”，以查询适合您的安全电邮解决方案。

[image]

返回：[image]这些使用暗网的人是如何被抓到的？: 总结教训

大多数电子邮件提供商都要求进行手机认证，这意味着您需要提供手机号码，在注册过程中验证短信会发送到您的手机以确认您的身份。

如果您使用的是一次性手机，仍然可以使用这些服务。但是，您必须安全地获取一次性手机和任何充值卡 —— 使用现金，通过一个无法追踪你的第三方购买。

另外，一旦获得了一次性手机，就不能在靠近您拥有的其他任何蜂窝设备的地方使用它。重申：将您的个人手机放在家里。

为了在网上购买比特币，您至少需要两个匿名创建的电子邮箱地址和比特币钱包。

所以现在，您已经有了一台装载Tor和Tails的笔记本电脑、一部一次

性手机、一些匿名的预付费礼品卡，但仍然没有万事俱备。

为了维持匿名性，您需要将匿名购买的预付费礼品卡变成加密货币。

[image]

第五步：将礼品卡变成比特币并进行清洗

一些加密货币，比如比特币，本身并不是匿名的，它们很容易通过区块链追溯到购买源，而后续的所有购买行为也都可以追溯到。于是，您必须让资金通过一个匿名机制：将预付费礼品卡转换成比特币，然后让这些比特币经过一个洗币服务。

这个过程会让您得到经过匿名化的加密货币，用于未来的支付。比如支付VPN、为一次性手机充流量。

您可以使用Tor在钱包网站上设置一个初始化钱包。一些网站中间商交易允许您使用预付费礼品卡购买比特币，比如 Vanilla Visa和Vanilla MasterCard 礼品卡。这种做法的缺点是，您需要为该服务支付至少 50%的高额溢价。

[image]

返回：[image]绕开KYC 的情况下用加密货币交换加密货币的方法

返回 - 对抗性思考方式：[image]调查区块链上的交易

洗钱一直以来都是罪犯做的事，最常见于贩毒活动中，它也在白领金融犯罪中发挥作用。但是，当政府将任何不服从均视为犯罪时，洗钱就是异议人士和反抗者不得不采取的行动。

洗钱意味着掩盖资金的原始所有权，通常的做法是将钱转移出国，转到其他有严格隐私法律的国家的多家银行。事实证明，您也可以对虚拟货币做类似的事。

有一种被称为混币的服务，可以将来自多个不同来源的加密货币混合在一起，这样得到的加密货币保留了它的价值，却携带了许多所有者的痕迹。这会使得之后人们难以确定某个特定的购买活动究竟是由哪个所有者做出的。但您必须非常小心谨慎，因为这方面的骗局多如牛毛。

我碰过运气。我在网上发现了一个洗币服务，会从交易中收取额外的费用。我实际上已经得到了我需要的等值比特币。但想想看这个情况：这个洗币服务现在知道我的一个匿名电子邮箱地址和在该交易中使用的两个比特币地址。所以为了进一步混淆，我将这些比特币又发送到了另一个比特币钱包，这个钱包是通过一个新的 Tor环路设置的，在我和我想访问的网站之间建立了新的跳跃。

现在，这个交易已经彻底模糊不清了，让人非常难以顺藤摸瓜地发现这两个比特币地址是同一个人所有。

当然，这个比特币洗币服务可以提供这两个比特币地址，从而与第三方合作。这就是安全地购买预付费礼品卡如此重要的原因。

在使用礼品卡购买了比特币之后，记得要安全地处理这些卡，不要丢在您家的垃圾桶里。推荐使用可用于塑料卡片的粉碎型碎纸机，然后将这些碎屑丢到远离您家或办公室的某个随机的垃圾桶里。

一旦您收到了洗过的比特币，你就可以注册一个以隐私优先的 VPN服务。

当您试图匿名的时候，最好的策略就是，不要相信任何 VPN提供商，包括那些宣称不会保留任何日志的提供商。

[image]

返回：[image]匿名托管服务VPS

您需要用洗过的加密货币通过 **Tor**浏览器来购买 **VPN**服务，或**VPS**。

建议查阅一下各家提供商的服务条款和隐私政策，并找到其中看起来最好的那个。

[image]

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

返回：[image]如何检查您的VPN连接是否实际加密

现在，您有了一台单独的笔记本电脑，上面同时运行着 Tor和 Tails，连接到了一个匿名购买的热点，用着洗过的加密货币购买的 VPN 服务，此外，还有甚至更多洗过的加密货币供应，那么到此，您就已经完成了最简单的部分—— 设置。

现在，进入困难的部分—— 维持匿名。

[image]

第六步：如果匿名性受损，那就再匿名一次

如果您在家使用了匿名热点，或者在使用您的匿名身份的实际位置打开了真实身份的个人手机、平板电脑或其他蜂窝设备，那么上述刚刚完成的所有设置和过程都会在一瞬间失去价值。

您只要一次犯错的机会，取证调查者就可以通过分析蜂窝提供商的日志，知道您曾出现在某个位置。

如果您的蜂窝设备总是在同一时间注册到同一手机基站，那么这种匿名接入就会呈现出某种模式，可能会导致您的真实身份被揭露出来。

现在，如果您的匿名性已经受损，而您决定进行另一个匿名活动，那么可能就需要再一次完成这个流程—— 在您的匿名笔记本电脑上清空数据并重新安装操作系统，创建另一套匿名电子邮箱账号和加密货币钱包，以及购买另一个匿名热点。

斯诺登和劳拉·珀特阿斯两人原本都已经有匿名的电子邮箱账号了，但他们还是设置了另外的备用账号，以专门用于彼此之间的通信。

只有当您怀疑自己原本已经建立的匿名性受损时，这种做法才有必要。

如果没必要，那您可以通过匿名的热点和 VPN来使用 Tor浏览器（在建立了一个新的 Tor环路之后），用一个不同的身份访问互联网。

当然，在这些建议中，选择遵循多少完全取决于您。

第七步：随机改变您的正常打字节奏

即使您遵循了这些建议，另一端的某个人仍然有可能识别出您。如何？—— 通过您打字的方式和语言风格。

[image]

返回：建议高风险学习者从“威胁知识库”相关专题进入 - [image]语言指纹

人们在写电子邮件或评论社交媒体帖子时会选择特定的词，关注这方面的研究相当多。通过检查这些词，研究者往往可以识别出你的性别和种族。

在第二次世界大战期间，英国政府在全国各地设立了一些监听站，来截听来自德国军方的信号。让盟军解码这些消息的进展来得迟了一点—— 在政府密码学校（ Government Code and Cypher School ）所在的布莱切利园，德国的 Enigma 密码被成功破解。早些时候，在布莱切利园截听德国电报消息的人可以根据点和画之间的距离识别出一个发送者的某些特征。比如，他们可以识别出何时出现了一个新的电报操作员，甚至还开始为这些操作员起名字。

简简单单的点和线如何揭示出背后的人？

是这样的，发送者按下一个键和再次按下这个键的时间间隔是可以测量出来的。这种区分方法之后被称为“发报指纹”（ Fist of the Sender）。

不同的莫尔斯电码按键操作员可以根据他们独特的“指纹”而被识别出来。电报本身并不是为这个目的设计的（谁关心发送消息的人是谁；消息是什么才重要），但是在这个案例中，独特的按键方式是一个有趣的副产品。

今天，随着数字技术的发展，电子设备可以测量出每个人在计算机键盘上的按键方式的纳米级差异—— 不仅是给定一个键被按下的时间长度，还有接下来一个键按下的速度。它可以区分普通打字的人和看着键盘打字的人。

将其与人们的词汇选择结合到一起，就可以揭示出很多有关一场匿名通信的信息。

如果您已经完成了匿名化您的 IP地址的麻烦的步骤，那么问题就会出现在这里。网络另一边的网站仍然可以识别您——不是因为某些技术上的东西，而是因为某些人类独有的东西。也称为行为分析。

假设某个使用 Tor匿名化的网站决定追踪你您按键档案。也许它背后的人是恶意的，目的就是了解更多有关您的信息。或者他们正在与政府间谍合作。

很多金融机构已经在使用按键分析来进一步验证账号持有人的身份了。这样就算某个人确实拿到了您的用户名和密码，他也没法伪造您的打字节奏。

当您需要在网上进行身份验证时，这是很可靠的。但如果您不想呢？因为部署按键分析非常简单，这很让人不安，所以研究人员创造了一个名叫 Keyboard Privacy 的浏览器插件。

这个插件会缓存您的个人按键，然后以不同的时间间隔将它们放出来。其中的思想是，为您的正常按键节奏加入随机性，从而在网络上实现匿名。这个插件也许可以进一步掩盖您的匿名互联网活动。

[image]

第八步：时刻保持警惕

您已经看到了，让真实生活和在网上的匿名生活之间保持隔离是可能的，但这需要时刻保持警惕。

我们曾经讨论过很多隐身失败的显著案例，那都是一些亮眼的，但持续时间很短的隐身尝试。

在 Ross Ulbricht ios的案例中，他没有真正谨慎地计划自己的替代身份，还偶尔使用他的真实电子邮箱地址，而不是匿名的电子邮箱地址，尤其是在开始的时候。通过使用谷歌高级搜索，一位调查者成功地将足够多的碎片信息组合到一起，从而揭露出 “丝绸之路” 的神秘所有者。

是的，一个“小错误”就能让您结束一切。保持住并不容易，除非您对细节有惊人的关注，否则真的很难过两种生活。

以下是一个著名的案例。

[image]

返回：[image]当您准备像编程随想那样工作…：须知

安全行业有一个真理：只要时间和资源足够，一个坚持不懈的攻击者终会成功。而您为试图实现自己的匿名而做的所有事情，实际上是在设置很多障碍，从而让攻击者放弃，并转向另外的目标。本站S04系列将更详细介绍这一原理。

大多数人只需要隐藏一小段时间。为了避免老板将您解雇；为了避免

前任的律师找到某些或任何可以利用的对您不利的东西；为了避开那些在社交网络上看到您的照片后决定骚扰您的可怕的跟踪狂；为了躲开政府间谍的滋扰 ……

不管您隐身的原因是什么，这里已经列出的步骤将在相当长的时间内帮助您摆脱困境。

在当今的数字世界中，匿名需要大量工作和持续不断的警惕。每个人对匿名的需求都不一样—— 您需要保护密码，让私密文件不被您的同事看到吗？需要躲避一个正在跟踪您的变态吗？如果您是一位敢于说出真相的人，您需要躲避执法部门和政府间谍吗？

您的个人需求决定了您需要采取的必要步骤，以便维持您想要的匿名水平—— 从设置强密码和意识到办公室的打印机可能对您不利，一直到完成这里给出的详细步骤，从而让取证调查者极难发现您的真实身份。

但总体而言，您至少可以了解到一些东西，从而帮助您最小化在数字世界中的痕迹。

在将背景中可以看到家庭地址的照片发布出去之前、在社交媒体资料上提供真实的生日和其他个人信息之前、在不使用 HTTPS Everywhere 扩展浏览互联网之前、在没有使用 Signal 这样的端到端加密工具拨打机密电话或发送短信之前 …… 在不使用 OTR 而是通过 AOL、 MSN Messenger 或 Google Talk 向一位重要人士发送消息之前，在不使用 PGP或 GPG发送机密电子邮件之前 …… 请三思。

我们可以积极主动地思考自己的信息，并且认识到，即使对正在做的事情感觉良好—— 分享照片、忘记修改默认登录名和密码、使用工作手机处理个人消息或为孩子设立 Facebook 账号，您所做的任何决定都有可能影响终身。

所以，需要行动起来。每个人（从对技术束手无策的人到专业的安全专家）都应该采取实际行动，掌握这门每天都在变得更为重要的技艺：隐身。

[image]
💯

训练-SelfDirectedTraining

正视所有恐惧、愤怒和不适，然后才能建设性修正。 Amateurs practice until they get it right, professionals practice until they can’t get it wrong.

[image]
[image]

S01E01-T2 识别威胁并作出反应

[image] 关键词	判断力 威胁响应
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025年3月3日
[image] **Description**	练习

[image]

这个练习是帮助您了解自己的认知在哪些领域是准确的、哪些不够清晰。

您应该对以下方面有更清晰的认识：

- 您过去对威胁的反应是什么样的，不管是顺利的还是不顺利的都包括；
- 在威胁识别方面您认为自己目前的水平与理想状态之间是否存在差距？是什么样的差距；
- 在威胁感知方面，您希望改变哪些事情来提升自己的敏锐度和准确度？
- 您认为可以去做点什么以帮助您更有信心面对新的威胁吗？- 或者，为此应该坚持什么？

回想一下您过去感到特别不安全的经历，然后采取行动来保护自己。虽然这种经历可能主要是身体上、情感上或与信息安全有关的，但它也可能对您的安全的其他方面产生了额外的影响。

使用下面这些问题来记录您的见解。

选择一个您会感到危险并需要采取行动保护自己的时刻。考虑身体上的危险经历（如黑头套）、情感上的伤害经历（如受到威胁或背叛）或对您的信息和通信的威胁（如设备被警察没收或电话被窃听），然后回答问题：

1、您是如何意识到威胁的？

2、是否有较早的迹象表明您注意到或可能没有注意到威胁？在社会政治环境、物理环境、设备以及身心等各方面考虑指标。

3、之前是否有迹象表明您已经注意到威胁，但是认为它并不重要？在社会政治环境、物理环境、设备以及身心等各方面考虑指标。

4、当您意识到威胁时，您最初的反应是什么？这些反应有多有效？

5、您接下来的行动是什么？这些措施的效果如何？

6、如果您可以回到过去，您会怎么做？

7、您可以从这种经验中学到什么，这些经验可以使您对自己应对未来困难的能力更有信心吗？

[image]
[image]

S01E01-T2 识别威胁并作出反应

[image] 关键词	判断力 威胁响应
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025/03/03
[image] **Description**	练习

[image]

这个练习是帮助您了解自己的认知在哪些领域是准确的、哪些不够清晰。

您应该对以下方面有更清晰的认识：

- 您过去对威胁的反应是什么样的，不管是顺利的还是不顺利的都包括；
- 在威胁识别方面您认为自己目前的水平与理想状态之间是否存在差距？是什么样的差距；
- 在威胁感知方面，您希望改变哪些事情来提升自己的敏锐度和准确度？
- 您认为可以去做点什么以帮助您更有信心面对新的威胁吗？- 或者，为此应该坚持什么？

回想一下您过去感到特别不安全的经历，然后采取行动来保护自己。虽然这种经历可能主要是身体上、情感上或与信息安全有关的，但它也可能对您的安全的其他方面产生了额外的影响。

使用下面这些问题来记录您的见解。

选择一个您会感到危险并需要采取行动保护自己的时刻。考虑身体上的危险经历（如黑头套）、情感上的伤害经历（如受到威胁或背叛）或对您的信息和通信的威胁（如设备被警察没收或电话被窃听），然后回答问题：

1、您是如何意识到威胁的？

2、是否有较早的迹象表明您注意到或可能没有注意到威胁？在社会政治环境、物理环境、设备以及身心等各方面考虑指标。

3、之前是否有迹象表明您已经注意到威胁，但是认为它并不重要？在社会政治环境、物理环境、设备以及身心等各方面考虑指标。

4、当您意识到威胁时，您最初的反应是什么？这些反应有多有效？

5、您接下来的行动是什么？这些措施的效果如何？

6、如果您可以回到过去，您会怎么做？

7、您可以从这种经验中学到什么，这些经验可以使您对自己应对未来困难的能力更有信心吗？

[image]
[image]

S01E01-T3 创伤经历如何影响您的认知

[image] 关键词	创伤 判断力 压力 威胁响应
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025年3月3日
[image] **Description**	练习

[image]

本练习的目的是帮助您识别最准确的感知区域、以及由于创伤经历而可能导致认识不清晰的区域。

花点时间来思考这些问题，并清楚地写下您的答案，这样随着时间的推移和自我意识的加深，您就可以回想这些问题。

请注意把您的笔记放在私密的地方，只与您信任的人分享您的个人想法和问题。

回想过去任何可能尚未完全解决的创伤经历。那些您经常会想到的经历，它们仍然在某种程度上让您感到害怕、愤怒、内疚、羞愧或悲伤。不要深究实际情况，而是专注于您为帮助自己所做的事、为帮助他人所做的事，以及他人为帮助您所做的事或可能做的事。

请考虑以下问题：

- 过去的经历给您带来了什么样的危险情况？
- 当您发现自己处于潜在危险的环境中时，是否有任何情况会使您很容易焦虑或害怕？
- 是否有您信任的人可以帮助您识别任何毫无根据的恐惧？
- 您感觉自己无法轻松识别哪些类型的威胁？
- 您将如何检查自己是否未能识别某些危险指标？
- 您觉得与谁讨论您的恐惧和可能出现的盲点更合适一些？

由于这个练习可能会对情绪造成挑战，因此要向您的合作者/同伴清楚地说明这一点。重要的是，不要让您的同伴觉得自己是被强迫参加这项活动的，如果有人开始感到痛苦，应立即停止。

将其与其他练习活动联系起来将产生更好的效果，因为这些练习都属于社会心理健康的领域。

花点时间做这些练习，把您的答案写清楚是很有帮助的，这样在您加深自我意识的时候，就可以回过头来看它们。

再次强调，要把您的笔记放在一个私密的地方，只与您信任的人分享您的个人想法和问题。

[image]
[image]

S01E01-T1 反思现有的安全实践

[image] 关键词	个人 团队 整体 防御
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025年3月3日
[image] **Description**	练习

[image]

这个练习可以帮助您反思安全对您的意义，并探索您以前有意识或无意识采取的安全战术、计划和策略，是否有更新的必要性。

通过本练习，您会对您现有的做法有一个快速的审视，它们是如何相互影响的，以及您如何利用它作为下一步的基础。

不论是个人练习和社区团队的分组讨论，都是好的；您可以把答案写在便签上，或者白板上。

问自己或小组以下问题：

1. 考虑下 “安全” 或 “安全性” 这个词，这实际上对您意味着什么？您需要在什么情况下/需要哪些东西，才能感到安全？

1. 您每天都在做哪些事以避免危险，并保护自己、自己的财产、朋友或家人？

1. 最近一次您作出的能使自己感到安全和坚强的事，是什么时候？

1. 回忆您进行的危险活动。为了安全起见，您做了什么？

1. 还有哪些其他人在帮助您感到安全方面是重要的？

1. 哪些资源或活动在帮助您感到安全方面是重要的？

请注意您对这些问题的答案，因为它们在以后的练习和指南的各部分中将很有用，并且会提醒您：您并不是在从头开始构建新的实践。

—— 备注与技巧 ——

如果目前没有谈论“安全”问题的组织文化，同事或团队成员可能会感到奇怪。不过，可以利用这个练习来开始这样一个提高认识的过程。

练习本身可能会开始产生有关改善或增加安全的实务想法。您可能希望将这些想法记录下来，为接下来的章节中介绍的规划做准备。

[image]
[image]

S01E01-T1 反思现有的安全实践

[image] 关键词	个人 团队 整体 防御
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025/03/03
[image] Description	练习

[image]

这个练习可以帮助您反思安全对您的意义，并探索您以前有意识或无意识采取的安全战术、计划和策略，是否有更新的必要性。

通过本练习，您会对您现有的做法有一个快速的审视，它们是如何相互影响的，以及您如何利用它作为下一步的基础。

不论是个人练习和社区团队的分组讨论，都是好的；您可以把答案写在便签上，或者白板上。

问自己或小组以下问题：

1. 考虑下 “安全” 或 “安全性” 这个词，这实际上对您意味着什么？您需要在什么情况下/需要哪些东西，才能感到安全？

1. 您每天都在做哪些事以避免危险，并保护自己、自己的财产、朋友或家人？

1. 最近一次您作出的能使自己感到安全和坚强的事，是什么时候？

1. 回忆您进行的危险活动。为了安全起见，您做了什么？

1. 还有哪些其他人在帮助您感到安全方面是重要的？

1. 哪些资源或活动在帮助您感到安全方面是重要的？

请注意您对这些问题的答案，因为它们在以后的练习和指南的各部分中将很有用，并且会提醒您：您并不是在从头开始构建新的实践。

—— 备注与技巧 ——

如果目前没有谈论 “安全” 问题的组织文化，同事或团队成员可能会感到奇怪。不过，可以利用这个练习来开始这样一个提高认识的过程。

练习本身可能会开始产生有关改善或增加安全的实务想法。您可能希望将这些想法记录下来，为接下来的章节中介绍的规划做准备。

[image]
[image]

S01E01-T3 创伤经历如何影响您的认知

[image] 关键词	创伤 判断力 压力 威胁响应
[image] 关联	[image]头疼医头是不够的：整体安全S01E01- 什么是‘整体’？如何‘安全’？
[image] 创建时间	2025/03/03
[image] **Description**	练习

[image]

本练习的目的是帮助您识别最准确的感知区域、以及由于创伤经历而可能导致认识不清晰的区域。

花点时间来思考这些问题，并清楚地写下您的答案，这样随着时间的推移和自我意识的加深，您就可以回想这些问题。

请注意把您的笔记放在私密的地方，只与您信任的人分享您的个人想法和问题。

回想过去任何可能尚未完全解决的创伤经历。那些您经常会想到的经历，它们仍然在某种程度上让您感到害怕、愤怒、内疚、羞愧或悲伤。不要深究实际情况，而是专注于您为帮助自己所做的事、为帮助他人所做的事，以及他人为帮助您所做的事或可能做的事。

请考虑以下问题：

- 过去的经历给您带来了什么样的危险情况？

- 当您发现自己处于潜在危险的环境中时，是否有任何情况会使您很容易焦虑或害怕？

- 是否有您信任的人可以帮助您识别任何毫无根据的恐惧？

- 您感觉自己无法轻松识别哪些类型的威胁？

- 您将如何检查自己是否未能识别某些危险指标？

- 您觉得与谁讨论您的恐惧和可能出现的盲点更合适一些？

☝

由于这个练习可能会对情绪造成挑战，因此要向您的合作者/同伴清楚地说明这一点。重要的是，不要让您的同伴觉得自己是被强迫参加这项活动的，如果有人开始感到痛苦，应立即停止。

将其与其他练习活动联系起来将产生更好的效果，因为这些练习都属于社会心理健康的领域。

花点时间做这些练习，把您的答案写清楚是很有帮助的，这样在您加深自我意识的时候，就可以回过头来看它们。

再次强调，要把您的笔记放在一个私密的地方，只与您信任的人分享您的个人想法和问题。

[image]
[image]

S01E02-T2 练习非暴力沟通和反馈

[image] 关键词	创伤 压力 团队 沟通
[image] 关联	[image]“抓特务” 不是解决方案：整体安全S01E02- 威胁响应
[image] 创建时间	2025/03/04
[image] **Description**	练习

[image]

本练习的目的是练习非暴力沟通，作为提高团队和小组内部安全问题沟通效率的一种手段。它提供了一个反思的机会，让我们思考如何以清晰易懂的方式提供反馈，避免一些可能导致争论或无效沟通的陷阱。

该练习最好先以两人一组的方式进行，但也可以调整为更大的群组。

在活动挂图等可见的地方张贴「非暴力反馈准则」可能会很有用。

决定进行反馈讨论的环境（可以两人一组，或与观察员轮流进行）。参与者应选择一个自己想要提供反馈的主题（真实的或想象的都可以）。这可以是一个与安全有关的话题，例如已经发生的事，或者是其他完全不同的话题。

请提供反馈的参与者遵循以下准则。对于每条准则，都会给出一个小的说明性例子。在这里，我们想象的是一个两人谈话的场景：其中一个同事经常加班到很晚，有一次离开办公室时忘了锁门；另一个同事想谈谈这件事。

接受反馈的人只能提出一些澄清的问题，而不能对反馈的内容进行评论、回复、辩解或质疑。

非暴力反馈指南

1、“我为我自己说话” —— 您只能根据自己的主观经验说话，而不能随意描述为 “常识”、“我的团队”、“我们” 或 “某人”，而只能说 “我”。

例子：“当我发现办公室门大敞着时，我感到不安全”。

不良做法：“你昨天所做的事使我们所有人处于危险之中！”

2、“你观察到了什么？” —— 您只应在经历事实时讲这些事实，这样对话者才能知道您的反馈所指的是什么（您所看到、听到的等等）。

例子：“今天早上我到达办公室时，前门是开着的，没用钥匙我就进来了”。

不良做法：“昨天是你忘了锁门！”

3、“您对此有何反应？” —— 您对自己的经历有什么内在感受和身体反应？尽量不要评论它，但再一次，只要从您的经验中了解就可以了。

例子：“我非常担心，害怕我们已经被抢劫了。当我发现一切正常时，我仍然很生气。”

4、“您如何解释它？” —— 您的个人解释为事实带来了什么？尽管您的个人解释确实是主观的，但它仍然很有价值，可以丰富您的经验。

例子："我认为发生这种情况是因为您工作很晚了，很累，只是忘了锁门"。

5、"您的愿望、建议或兴趣是什么？" —— 根据这种经验，您对变更有何建议？应无要求地提供这些信息。

例子："如果我们都能得到足够的休息、不会过度劳累，那么我会感觉更好，以便我们能够更好地照顾到类似锁门这种细节的但比较重要的事情，所以如果您不工作到这么晚会更好。"

然后请两人分享他们对反馈过程和方式的见解 —— 而不是内容。他们是否体验到与平时接受反馈时不同的感受？

此练习还可以用于阐明反馈的内容和语气，为实际的反馈讨论或可能困难的讨论做准备。

中国朋友可以选择您所在的安全群组，尝试这些练习；更好的是与您的同伴面对面尝试这些练习，它或许有希望将群聊升级为社区。

备注与技巧 ——

重要的是用您的耳朵而不是用嘴巴，来接受反馈，并将其理解为您的队友的个人反映，而不是"真相"或刺激你为自己的行为辩护。

您自己来决定它是否对您有价值，以及如何对它作出反应。遵循这样的方法可能是预防团队内部冲突的一个步骤。因此，它可以促进你们的整体福祉。

[image]
[image]

S01E02-T2 练习非暴力沟通和反馈

[image] 关键词	创伤 压力 团队 沟通
[image] 关联	[image]“抓特务” 不是解决方案：整体安全S01E02- 威胁响应
[image] 创建时间	2025年3月4日
[image] **Description**	练习

[image]

本练习的目的是练习非暴力沟通，作为提高团队和小组内部安全问题沟通效率的一种手段。它提供了一个反思的机会，让我们思考如何以清晰易懂的方式提供反馈，避免一些可能导致争论或无效沟通的陷阱。

该练习最好先以两人一组的方式进行，但也可以调整为更大的群组。

在活动挂图等可见的地方张贴「非暴力反馈准则」可能会很有用。

决定进行反馈讨论的环境（可以两人一组，或与观察员轮流进行）。参与者应选择一个自己想要提供反馈的主题（真实的或想象的都可以）。这可以是一个与安全有关的话题，例如已经发生的事，或者是其他完全不同的话题。

请提供反馈的参与者遵循以下准则。对于每条准则，都会给出一个小的说明性例子。在这里，我们想象的是一个两人谈话的场景：其中一个同事经常加班到很晚，有一次离开办公室时忘了锁门；另一个同事想谈谈这件事。

接受反馈的人只能提出一些澄清的问题，而不能对反馈的内容进行评论、回复、辩解或质疑。

非暴力反馈指南

1、“我为我自己说话” —— 您只能根据自己的主观经验说话，而不能随意描述为 “常识”、“我的团队”、“我们” 或 “某人”，而只能说 “我”。

例子：“当我发现办公室门大敞着时，我感到不安全”。

不良做法：“你昨天所做的事使我们所有人处于危险之中！”

2、“你观察到了什么？” —— 您只应在经历事实时讲这些事实，这样对话者才能知道您的反馈所指的是什么（您所看到、听到的等等）。

例子：“今天早上我到达办公室时，前门是开着的，没用钥匙我就进来了”。

不良做法：“昨天是你忘了锁门！”

3、“您对此有何反应？” —— 您对自己的经历有什么内在感受和身体反应？尽量不要评论它，但再一次，只要从您的经验中了解就可以了。

例子：“我非常担心，害怕我们已经被抢劫了。当我发现一切正常时，我仍然很生气。”

4、“您如何解释它？” —— 您的个人解释为事实带来了什么？尽管您的个人解释确实是主观的，但它仍然很有价值，可以丰富您的经验。

例子：“我认为发生这种情况是因为您工作很晚了，很累，只是忘了锁门”。

5、“您的愿望、建议或兴趣是什么？” —— 根据这种经验，您对变更有何建议？应无要求地提供这些信息。

例子：“如果我们都能得到足够的休息、不会过度劳累，那么我会感觉更好，以便我们能够更好地照顾到类似锁门这种细节的但比较重要的事情，所以如果您不工作到这么晚会更好。”

然后请两人分享他们对反馈过程和方式的见解 —— 而不是内容。他们是否体验到与平时接受反馈时不同的感受？

此练习还可以用于阐明反馈的内容和语气，为实际的反馈讨论或可能困难的讨论做准备。

中国朋友可以选择您所在的安全群组，尝试这些练习；更好的是与您的同伴面对面尝试这些练习，它或许有希望将群聊升级为社区。

备注与技巧 ——

重要的是用您的耳朵而不是用嘴巴，来接受反馈，并将其理解为您的队友的个人反映，而不是 “真相” 或刺激你为自己的行为辩护。

您自己来决定它是否对您有价值，以及如何对它作出反应。遵循这样的方法可能是预防团队内部冲突的一个步骤。因此，它可以促进你们的整体福祉。

[image]
[image]

S01E02-T1 团队会议安全议题模版

[image] 关键词	会议 团队 防御
[image] 关联	[image]“抓特务” 不是解决方案：整体安全S01E02- 威胁响应
[image] 创建时间	2025年3月4日
[image] **Description**	练习

[image]

本练习的目的是帮助您思考如何以及何时与同伴、同事或团队谈论安全问题。本练习最好由两个或以上人协助进行，当然也可以把它作为您与同事互动时的有用的个人思考工具。

这个练习有助于在您的团队/小组中开始一个建设性地谈论和讨论安全问题的过程。

为了以参与的方式进行练习并记录下来，您可能需要一些书写材料 —— 卡片或便签和做标记的东西；大面的墙面空间，活动挂图也可能有用。

步骤1：将您的组织分成两人一对的组合。让每一对成员都考虑以下有关组织动态的问题，并写下答案：

1. 在组织对话中，哪些主题占据了大部分时间？

1. 在组织内讨论中，哪些话题我们几乎没有涉及到？在组织互动中的哪些方面会让我们感到振奋？

1. 在小组互动的哪些方面会让我们感到疲惫不堪？冷场，难以进行下去？

1. 当人们意见分歧时，组织会发生什么？

1. 您的团队是否为个人创造了发展和完善自己的安全实践的空间？描述一下：这个空间何时何地存在？是否足够？如果需要，您将如何扩展此空间？

1. 您是否有足够的空间与他人（例如与您紧密合作的同事或队友）谈论安全问题，以及在必要时如何创建或扩展此空间？

步骤2：在挂板上或笔记本上整理对这些问题的完整答案。

步骤3：请作为一个团队考虑以下问题：

1. 我们要在哪里以及如何确定安全方面的优先事项？

1. 将安全作为一个整体进行讨论会引起哪些常见问题？

1. 什么东西会妨碍我们谈论安全性？我们该如何处理？

1. 我们如何才能创造和维持足够的空间来谈论安全问题？就时间和资源而言，这意味着什么？

1. 我们如何提高组织内互动在安全性方面的效力？

1. 致力于更改现有的安全实践会出现什么问题吗？我们是否正在

抵制改变，不论是个人还是群体，为什么？

步骤4：邀请每个人思考下面的问题：

1. 您是否应该追求在家人和熟人圈子里普及类似程度的安全意识？

1. 当危险出现时，您的家人和熟人受到影响的方式会有什么不同吗？

1. 您以什么方式传达您的敏感工作可能招致的威胁对您的家人、社区、朋友和不在工作圈内的其他人的影响？

步骤5：在整个团队中，分享那些人们觉得可以自由分享的观点：

然后，你应该同意出于安全的原因，哪些内容可以传达给小组以外的人。为整个小组商定这些准则。

备注和技巧 ——

还应考虑讨论必要的步骤和要求，以便将您关于未来如何谈论安全问题的想法付诸实践。需要思考的重要问题可能包括：

- 如果你们的讨论没有取得进展，会怎样？

- 如果你们中有人不遵守规则泄漏了你们的讨论，会发生什么？

准备好您的答案。

[image]
[image]

S01E02-T1 团队会议安全议题模版

[image] 关键词	会议 团队 防御
[image] 关联	[image]“抓特务” 不是解决方案：整体安全S01E02- 威胁响应
[image] 创建时间	2025/03/04
[image] Description	练习

[image]

本练习的目的是帮助您思考如何以及何时与同伴、同事或团队谈论安全问题。本练习最好由两个或以上人协助进行，当然也可以把它作为您与同事互动时的有用的个人思考工具。

这个练习有助于在您的团队/小组中开始一个建设性地谈论和讨论安全问题的过程。

为了以参与的方式进行练习并记录下来，您可能需要一些书写材料 —— 卡片或便签和做标记的东西；大面的墙面空间，活动挂图也可能有用。

步骤1：将您的组织分成两人一对的组合。让每一对成员都考虑以下有关组织动态的问题，并写下答案：

1. 在组织对话中，哪些主题占据了大部分时间？

1. 在组织内讨论中，哪些话题我们几乎没有涉及到？在组织互动中的哪些方面会让我们感到振奋？

1. 在小组互动的哪些方面会让我们感到疲惫不堪？冷场，难以进行下去？

1. 当人们意见分歧时，组织会发生什么？

1. 您的团队是否为个人创造了发展和完善自己的安全实践的空间？描述一下：这个空间何时何地存在？是否足够？如果需要，您将如何扩展此空间？

1. 您是否有足够的空间与他人（例如与您紧密合作的同事或队友）谈论安全问题，以及在必要时如何创建或扩展此空间？

步骤**2**：在挂板上或笔记本上整理对这些问题的完整答案。

步骤**3**：请作为一个团队考虑以下问题：

1. 我们要在哪里以及如何确定安全方面的优先事项？

1. 将安全作为一个整体进行讨论会引起哪些常见问题？

1. 什么东西会妨碍我们谈论安全性？我们该如何处理？

1. 我们如何才能创造和维持足够的空间来谈论安全问题？就时间和资源而言，这意味着什么？

1. 我们如何提高组织内互动在安全性方面的效力？

1. 致力于更改现有的安全实践会出现什么问题吗？我们是否正在

抵制改变，不论是个人还是群体，为什么？

步骤4：邀请每个人思考下面的问题：

1. 您是否应该追求在家人和熟人圈子里普及类似程度的安全意识？

1. 当危险出现时，您的家人和熟人受到影响的方式会有什么不同吗？

1. 您以什么方式传达您的敏感工作可能招致的威胁对您的家人、社区、朋友和不在工作圈内的其他人的影响？

步骤5：在整个团队中，分享那些人们觉得可以自由分享的观点：

然后，你应该同意出于安全的原因，哪些内容可以传达给小组以外的人。为整个小组商定这些准则。

备注和技巧 ——

还应考虑讨论必要的步骤和要求，以便将您关于未来如何谈论安全问题的想法付诸实践。需要思考的重要问题可能包括：

- 如果你们的讨论没有取得进展，会怎样？

- 如果你们中有人不遵守规则泄漏了你们的讨论，会发生什么？

准备好您的答案。

[image]
[image]

S01E03-T1 周围是谁？可视化人际关系图谱

[image] 关键词	关系 团队 战略策划 防御
[image] 关联	[image]知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者
[image] 创建时间	2025年3月5日
[image] Description	练习

[image]

本练习的想法是开始一个过程，以可视化您自己、您的团队或组织、以及您与周围其他参与者的关系，包括直接、间接和潜在的未来联系。

在这部分，建议您把重点放在头脑风暴上，想想您身边的行为者都是谁，以及您与他们的关系强度（直接、间接或潜在）。下一步就是扩展可视化或关系图谱，以包括您与他们的关系类型。

在团队中进行此练习时，您需要：

- 可以用来展示的挂板、白板
- 彩色信号笔或水笔
- 便签/便利贴

步骤如下。

写下或绘制可视化图谱

在本练习中建议您使用便签或便利贴，写上行为者的名字，以便在背景中直观地映射他们、以及他们之间的关系。

1、从您自己或您的组织作为一个实体开始，集思广益，确定尽可能多的与您的工作有关的行为者 —— 这可以包括个人、团体、组织或机构；必要时考虑地方、区域、国家和国际行为者。

2、您挂在墙上的这块板子的中心位置应该是您自己、和/或您的目标群体，如果他们是可识别的话，重要的行为者围绕在周围。

3、考虑这些分类：

- 直接的 —— 就您试图影响的问题与您直接接触的人、团体、组织、机构。例如，谁可能与您为之工作的目标群体有直接关系，还有一些直接反对您工作的实体，会直接挑战或对抗您的那些人。您也可以将您周围的社区成员加入进来，包括您的家人和朋友，他们可能以某种方式支持（也可能反对）您的工作。

- 间接的 —— 这些可以包括与您一步之遥的人、团体、组织或机构。在上面的例子中，对于与您有直接关系的目标团体，他们也很可能与其他人有直接关系，于是后者这些人就成为了与您的间接关系。

- 潜在的/外围的 —— 与您的目标问题有关的人、团体、组织和机构，但您（目前还）与他们没有联系或关系。这方面的例子包括支持您的问题、但在您的背景下并不积极的国际机构。

尽管您可能没有想到，但是您依然有必要将那些您需要依靠其来管理

信息和交流的行为者包含进去。这些可以是：

- 您的电话服务提供商
- 您的互联网服务提供商
- 社交媒体帐户提供商
- 电子邮件帐户提供商

在下一个练习中将更详细地探讨这些参与者。

备注 ——

接下来的内容将旨在扩展您对这些行为者的了解，并利用他们来建立对您所面临的威胁的分析。一旦您完成了这一练习，最好保留一份这些行为者的清单，供今后参考和阐述。

[image]
[image]

S01E03-T2 绘制行为者关系图谱

[image] 关键词	关系 团队 威胁模型 战略图谱
[image] 创建时间	2025年3月5日
[image] **Description**	练习

[image]

本练习是在上一个练习的可视化行为者图谱的基础上进行的，第一部分是在图谱上标明行为者之间的关系，确定盟友、对手和中立方；然后就是，利用第一步的结果来确定和分析您所处环境中可能代表有意（或无意）威胁来源的具体行为者。

“有意”威胁和“无意”威胁虽然在很多时候会导致同样的结果，但干预方式是不同的。

举例比如，对于网格员和“片儿警”来说，挖掘和确定监视目标是具体的“维稳指标”，它对应具体的经费额度（即他们的收益），理论上他们有很强的动机形成主动威胁；监视资本主义巨头公司也是如此，存在一个稳固的利益链条驱动他们形成伤害。对此很大程度上只能通过主动防御来降低风险，多想一步比没想到要好得多。

而“无意”威胁则更可能来自于近距离关系，比如一个被等级制和竞争支配文化充斥的社区/群体，就像在我们的Women's Day 2025研讨会中参与者的描述，暴露他人隐私只为证明自己的圈子地位，类似现象依然存在于某些异议群体内，这非常危险。对这种情况来说，改变方法是通过社区/团队中有足够高公信力的组织者和支持者一起拟定恰当的安全文化规则（对此我们将在后面详细描述），并同时通过修正社区文化以鼓励平等和彼此照护的关系结构。

更多相关策略和技巧本项目有单独栏目讲述 - “反渗透和协作”。

在本练习中您需要：

- 基本的行为者关系图谱（来自上一个练习）
- 纸和彩色记号笔或钢笔
- 彩色便利贴

步骤

考虑您和团队目前为止能想到的所有行为者：

1、根据这些行动者与您的工作之间的关系的性质 —— 盟友、对手、中立、未知 —— 来标注他们。您可以使用不同颜色的便利贴、或安排不同位置来实现，比如 盟友在左边、对手在右边、中立者在中间，这样会比较直观。

2、在这张图上的每个行为者周围画一个圆，其大小可以与其在社会政治背景下的权力和资源相对应。

3、把您自己放在这张图上，然后连线，将您与您有关系的任何行为者之间建立联系。

使用下面的示例表示这张图上的角色之间存在的不同类型的关系。包括：

- 亲密关系：行为者之间保持积极的关系，具有可靠的和稳定的互信互助；

- 联盟关系：参与者之间相互协调并共同行动，彼此；
- 弱关系或未知关系：几乎没有联系的关系，或者本质上性质未知的关系；
- 冲突关系：两个行为者之间有敌对关系；
- 暴力冲突关系：这种关系的特征是一方或双方都遭受身体（潜在武装）暴力；
- 从属关系：一个行为人对另一个行为人有权力，可以指挥他们做某事，例如 受武装部队控制的准军事集团、私人维稳公司等等；
- 相互依赖关系：两个实体以某种方式彼此绑定。

备注和技巧

定期重新审视并反思您创建的图谱，以及进行任何有必要的添加、删除、或更改，都是很有用的。一定要记得，定期进行重新评估和更新非常重要，尤其是在采取新的措施之前。

其他行为者信息图表

对于每一个盟友和对手 —— 请优先考虑积极的盟友和对手 —— 您可以详细说明他们与您的工作关系的性质，并建立一个信息表，提供关于他们的动机、他们的利益、他们与您的关系史、以及他们的资源（物质、财政、人脉或其他）的进一步信息。

该信息表将帮助您：

- 确定激发他们立场的潜在利益和关系。他们为什么和您站在一起？或者，为什么反对您？别怕说实话，说实话很重要，尤其是对于您的支持者的分析；

- 确定他们拥有和运用的资源和策略，这些资源和策略如何帮助您、或阻碍您的工作。

还应思考他们在更广泛的社会政治背景下的地位，以及他们可能从该地位中获得哪些特权和资源。

必须指出，这些动机和资源将随着时间的推移而变化。随着新信息的出现，您应该定期更新这一分析。此外，非常重要的是，要考虑信息来源的可信度：无论是通过个人接触、非正式关系网络、当地媒体还是其他。

[image]
[image]

S01E03-T1 周围是谁？可视化人际关系图谱

[image] 关键词	关系 团队 战略策划 防御
[image] 关联	[image]知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者
[image] 创建时间	2025/03/05
[image] Description	练习

[image]

本练习的想法是开始一个过程，以可视化您自己、您的团队或组织、以及您与周围其他参与者的关系，包括直接、间接和潜在的未来联系。

在这部分，建议您把重点放在头脑风暴上，想想您身边的行为者都是谁，以及您与他们的关系强度（直接、间接或潜在）。下一步就是扩展可视化或关系图谱，以包括您与他们的关系类型。

在团队中进行此练习时，您需要：

- 可以用来展示的挂板、白板
- 彩色信号笔或水笔
- 便签/便利贴

步骤如下。

写下或绘制可视化图谱

在本练习中建议您使用便签或便利贴，写上行为者的名字，以便在背景中直观地映射他们、以及他们之间的关系。

1、从您自己或您的组织作为一个实体开始，集思广益，确定尽可能多的与您的工作有关的行为者 —— 这可以包括个人、团体、组织或机构；必要时考虑地方、区域、国家和国际行为者。

2、您挂在墙上的这块板子的中心位置应该是您自己、和/或您的目标群体，如果他们是可识别的话，重要的行为者围绕在周围。

3、考虑这些分类：

- 直接的 —— 就您试图影响的问题与您直接接触的人、团体、组织、机构。例如，谁可能与您为之工作的目标群体有直接关系，还有一些直接反对您工作的实体，会直接挑战或对抗您的那些人。您也可以将您周围的社区成员加入进来，包括您的家人和朋友，他们可能以某种方式支持（也可能反对）您的工作。

- 间接的 —— 这些可以包括与您一步之遥的人、团体、组织或机构。在上面的例子中，对于与您有直接关系的目标团体，他们也很可能与其他人有直接关系，于是后者这些人就成为了与您的间接关系。

- 潜在的/外围的 —— 与您的目标问题有关的人、团体、组织和机构，但您（目前还）与他们没有联系或关系。这方面的例子包括支持您的问题、但在您的背景下并不积极的国际机构。

尽管您可能没有想到，但是您依然有必要将那些您需要依靠其来管理

信息和交流的行为者包含进去。这些可以是：

- 您的电话服务提供商
- 您的互联网服务提供商
- 社交媒体帐户提供商
- 电子邮件帐户提供商

在下一个练习中将更详细地探讨这些参与者。

备注 ——

接下来的内容将旨在扩展您对这些行为者的了解，并利用他们来建立对您所面临的威胁的分析。一旦您完成了这一练习，最好保留一份这些行为者的清单，供今后参考和阐述。

[image]
[image]

S01E03-T2 绘制人际关系图谱

[image] 关键词	关系 团队 威胁模型 战略图谱
[image] 关联	[image]知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者
[image] 创建时间	2025/03/05
[image] Description	练习

[image]

本练习是在上一个练习的可视化行为者图谱的基础上进行的，第一部分是在图谱上标明行为者之间的关系，确定盟友、对手和中立方；然后就是，利用第一步的结果来确定和分析您所处环境中可能代表有意（或无意）威胁来源的具体行为者。

“有意”威胁和“无意”威胁虽然在很多时候会导致同样的结果，但干预方式是不同的。

举例比如，对于网格员和“片儿警”来说，挖掘和确定监视目标是具体的“维稳指标”，它对应具体的经费额度（即他们的收益），理论上他们有很强的动机形成主动威胁；监视资本主义巨头公司也是如此，存在一个稳固的利益链条驱动他们形成伤害。对此很大程度上只能通过主动防御来降低风险，多想一步比没想到要好得多。

而“无意”威胁则更可能来自于近距离关系，比如一个被等级制和竞争支配文化充斥的社区/群体，就像在我们的Women's Day 2025研讨会中参与者的描述，暴露他人隐私只为证明自己的圈子地位，类似现象依然存在于某些异议群体内，这非常危险。对这种情况来说，改变方法是通过社区/团队中有足够高公信力的组织者和支持者一起拟定恰

当的安全文化规则（对此我们将在后面详细描述），并同时通过修正社区文化以鼓励平等和彼此照护的关系结构。

更多相关策略和技巧本项目有单独栏目讲述 - “反渗透和协作”。

在本练习中您需要：

- 基本的行为者关系图谱（来自上一个练习）
- 纸和彩色记号笔或钢笔
- 彩色便利贴

步骤

考虑您和团队目前为止能想到的所有行为者：

1、根据这些行动者与您的工作之间的关系的性质 —— 盟友、对手、中立、未知 —— 来标注他们。您可以使用不同颜色的便利贴、或安排不同位置来实现，比如 盟友在左边、对手在右边、中立者在中间，这样会比较直观。

2、在这张图上的每个行为者周围画一个圆，其大小可以与其在社会政治背景下的权力和资源相对应。

3、把您自己放在这张图上，然后连线，将您与您有关系的任何行为者之间建立联系。

使用下面的示例表示这张图上的角色之间存在的不同类型的关系。包括：

- 亲密关系：行为者之间保持积极的关系，具有可靠的和稳定的互信互助；

- 联盟关系：参与者之间相互协调并共同行动，彼此；

- 弱关系或未知关系：几乎没有联系的关系，或者本质上性质未知的关系；

- 冲突关系：两个行为者之间有敌对关系；

- 暴力冲突关系：这种关系的特征是一方或双方都遭受身体（潜在武装）暴力；

- 从属关系：一个行为人对另一个行为人有权力，可以指挥他们做某事，例如 受武装部队控制的准军事集团、私人维稳公司等等；

- 相互依赖关系：两个实体以某种方式彼此绑定。

备注和技巧

定期重新审视并反思您创建的图谱，以及进行任何有必要的添加、删除、或更改，都是很有用的。一定要记得，定期进行重新评估和更新非常重要，尤其是在采取新的措施之前。

其他行为者信息图表

对于每一个盟友和对手 —— 请优先考虑积极的盟友和对手 —— 您可以详细说明他们与您的工作关系的性质，并建立一个信息表，提供关于他们的动机、他们的利益、他们与您的关系史、以及他们的资源（物质、财政、人脉或其他）的进一步信息。

该信息表将帮助您：

- 确定激发他们立场的潜在利益和关系。他们为什么和您站在一起？或者，为什么反对您？别怕说实话，说实话很重要，尤其是对于您的支持者的分析；

- 确定他们拥有和运用的资源和策略，这些资源和策略如何帮助您、或阻碍您的工作。

还应思考他们在更广泛的社会政治背景下的地位，以及他们可能从该地位中获得哪些特权和资源。

必须指出，这些动机和资源将随着时间的推移而变化。随着新信息的出现，您应该定期更新这一分析。此外，非常重要的是，要考虑信息来源的可信度：无论是通过个人接触、非正式关系网络、当地媒体还是其他。

[image]
[image]

S01E04-T1 清点您最重要的信息资产

[image] 关键词	自检 防御
[image] 关联	[image]夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产
[image] 创建时间	2025/03/06
[image] **Description**	练习

[image]
[image]

S01E04-T1 清点您最重要的信息资产

[image] 关键词	自检 防御
[image] 关联	[image]夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产
[image] 创建时间	2025年3月6日
[image] **Description**	练习

[image]

本练习的目的是对您管理的最重要的信息资产进行清点，以便为以后的保管创建最有效策略。

要开始练习（尤其是在小组中进行时），可以使用电子表格、大张纸和便笺或其他一些能让团队轻松进行头脑风暴并将其组织在一起的方法。集思广益并列出您管理的所有数据。

如果不确定从哪里开始，请考虑：

- 与您的 每项 敏感行动有关的数据
- 个人 数据和文件，特别是存储在工作用计算机上的数据
- 在线浏览行为，尤其是敏感数据的在线浏览

- 与敏感活动有关的任何电子邮件、短信和其他形式的通讯

想象一个电子表格，其中有几列类别，如下所述；您的任务是在行中填充信息。从静态信息开始，对于每种类型的信息，请详细说明以下内容：

- 这是什么信息？
- 它驻留在哪里？
- 谁有权使用它？
- 它的敏感程度如何 —— 严格保密、机密、公开；
- 保留它有多重要？
- 谁有权使用它？
- 应该如何保护它？
- 销毁前应保存多长时间？

您可以重复相同的过程，并使用其他条目扩展电子表格。例如数据传输（物理的、电子的），通过互联网或电信网络的通信。下面的示例可供参考：

[image] [image]

请注意这只是关于框架的示例，无关具体的安全建议。

此过程是迭代的。完成第一轮后，您可以检测模式和分组。例如，您可能决定，由于所有财务信息（无论类型如何）都具有相似的敏感度和使用寿命，因此可以将它们分组到统一的“财务信息”类别。

相反，您也可能会发现自己需要将一行扩展为几行。例如，包含“电子邮件”的行需要扩展为几行，把敏感的部分电子邮件单独分出来，以匹配相应的安全保存方案。

这应该是一个实时更新的文档，并且会根据您所处环境的变化和发展而变化。定期检查此文档很重要。

此时，您已经拥有描述您/您的组织的信息生态系统的初始文档，该文档以及参与者的图谱在您开始了解自己的力量和弹性以及可能存在弱点的领域时，将非常宝贵。

然后，您可以开始绘制从已确定的安全指标到特定威胁场景，再到设计策略、计划、工具和方式的路径，这些路径可以帮助您避免这些类型的场景或将其影响最小化。

[image]
[image]

S01E05-T3 确认可能遭受的所有威胁

[image] 关键词	判断力 威胁模型
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025年3月7日
[image] Description	练习

[image]

这项工作是首次尝试确定对您自己、您的团体或组织、以及您的反抗行动的威胁。然后，可对这份初步威胁清单进行完善，以便更深入地关注最有可能出现的、或可能最有害的威胁。

从以下内容开始，本练习将更容易：

- 对您所处环境中正在进行的政治、经济、社会和技术趋势，进行分析；
- 为实现反抗目标而进行的活动或工作类型的列表；
- 您根据前文内容构建的“行为者图谱”，尤其是您的对手的关系图；
- 您在以前的工作中观察到的安全指标列表。

考虑并写下所有对您自己、您的组织和工作的潜在威胁。从您的每项活动或工作领域开始对它们进行分类，可能会有所帮助。

请记住：威胁是任何可能对您自己或您的工作造成伤害的潜在事件 —— 无论是政治方面还是其他方面。

编制一份这些威胁的清单。如果您觉得有困难，可以考虑您的对手以及他们过去对其他人权维护者采取行动的方式。分析您的安全指标，并考虑它们是否对您构成具体威胁。

观察在您所确定的威胁中出现的任何模式：这些威胁主要与您的某些活动有关，还是来自某些对手？这在进行安全规划时将会很有用 (即特别为某些活动进行规划，或为与某些行为者的接触方式制定专门的计划 —— 比如接受传唤和被查水表，是不同的)。

保留这份清单，以便在以下练习中进行分析。

如果清单有点长，思考这些潜在的威胁可能会让人不知所措。这也可能是一项具有挑战性的工作，因为人们可能不知道自己有多现实。做好这个心理准备。

重要的是要记住，政治威胁总是来自某个或一组行为者，他们认为自己的利益可能受到您的反抗的威胁。正如很多中国反抗者长期声明的那样：从某种意义上说，威胁是一个信号，表明您的努力是有效的，您的对手害怕您的存在。

虽然这可能是一个激发恐惧的时刻，但清楚地认识到您所面临的威胁也应该是一个增强力量的时刻。

承认这些威胁及其发生的可能性，可以帮助您更好地计划和可能减轻对您或您的工作造成的损害，如果其中任何一个威胁发生的话。

请记住，并非所有对您的安全威胁和心理压力都是出于政治动机或与您的反抗行动有关。威胁还可能来自轻微犯罪、基于性别的暴力和环

境危害，仅举几例。有时，正是这些威胁可能对人权维护者构成最大的风险。您需要清楚地识别状况。

必须提醒这点，人们对威胁的认识从来都不是完美的，不可太自信，但您可以改进它。如果您在自己的组织中进行练习，可能会有些其他队友说出了您以前没有想到的威胁，反之亦然。

在接下来的练习中，我们将提出一些问题，这些问题可能会帮助您批判性地思考您对威胁的看法，并制定策略，使您的看法更加准确。

您将学会识别自己的盲点和缺少的流程，以创建流程来填补这些空白。

向自己或您的组织询问以下问题：

1. 您是否曾经发现或其他人告知过您关于威胁的发生？那是您以前不知道的事吗？

1. 如果您是在小组中进行练习，那么其他人会对您提到的威胁感到惊讶吗？为什么？

1. 在您意识到威胁之前，您认为它们已经存在了多长时间了？

1. 您如何才能最快地意识到这些威胁？

1. 您如何在组织中与队友交流有关他们的信息？

1. 是什么使您的队友或多或少地感到事态严重？

1. 您能识别出比实际更为严重的威胁吗？为什么？

1. 如果您正在团队中进行这个练习，请考虑：以上答案的区别是什么？是什么让您和其他人以不同的方式想到同一威胁？

列出您面临的所有威胁可能会令人不知所措，会感觉很可怕。确保不要匆忙进行此练习，并留出空间让人们表达自己的感受。如果您认为此练习有用，请考虑使其成为常规 —— 每周或每月定期进行，以维护您的防御计划最新。

[image]
[image]

S01E05-T2监测自己的压力水平

[image] 关键词	压力监测 心理安全 自检
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025年3月7日
[image] Description	练习

[image] [image] [image]

人们很容易忽视自己的身体健康和心理健康，但健康的变化可能表明对外部问题的反应，如压力增加，这反过来又会影响您的安全状况—— 您会由于焦虑和压力失去敏锐的判断力。

敏感人士有时会逼迫自己继续工作，但这样做有可能随着时间的推移对您的健康造成持久的损害，进而阻碍您分析安全形势的能力。

您可能不习惯于监测自己的健康状况，而且变化可能是逐渐发生的，因此，开始对身体、情感和心理的变化进行记录是个好办法。其中一个方法就是做一个压力表，就像下面的练习这样。

这个练习可以帮助您找出自己在不同压力下的极限，如何认识这些极限和应对压力的措施。请花一些时间，最好是在没有压力的状况下尝试建立自己的压力表。

请停用任何成瘾物品 - 包括咖啡、浓茶、酒精饮品 - 至少**24**小时，再进行观察记录，将更接近真实的心理状态。

本练习将压力分为三个级别，就如交通信号灯：

绿色＝ 可承受的、能激发动力的压力。这种压力可能会让您保持创造力，但您可能会更容易疲惫，需要更多的休息时间，并且您知道自己不想长时间感受这种压力。

黄色＝ 令人不快的压力。在这种程度的压力下，您可能会感到疲惫，同时也会有所警觉。您可能会表现出压力的身体迹象（因人而异）。通常会有一种强烈的愿望，想要改变这种状况。

红色＝ 难以忍受的、深刻的和持久的压力。这种压力会影响您生活的不同领域，包括您的工作关系、与朋友和家人的关系、以及您的个人关系。这种程度的压力也降低了您从娱乐活动中获得的乐趣和放松，会感到焦虑和痛苦。身体会出现明显的生理反应 —— 常见的如偏头痛、心悸、失眠多梦等等，可能会感到接近崩溃，也许会采取不健康的措施来保持自己的警觉能力，如兴奋剂、易成瘾物品。

- 第1步：绘制一个初始压力表，并与您信任的人进行分析和思考。

- 第2步：决定一个固定的时间表，当您想检查和判断自己的压力状态和进行分析时。

- 第3步：如果您在一段时间内经常经历高压力状态，请检讨您的压力表，以确定它是否仍然足够。

这是帮助您及时地了解自己，避免“视而不见”或错误地归因。清晰的了解 —— 这对防御措施构建非常重要。

检查此压力表需要作为您的个人安全指南中的一个步骤，应定期进行。请确保检查您对不同级别的压力的定义是否仍然正确，或者，您是否已经对较高的压力级别习以为常。

[image]
[image]

S01E05-T1 制定检查清单

[image] 关键词	个人 团队 基准线 威胁识别
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025年3月7日
[image] **Description**	练习

[image]

这个练习的目的是帮助您通过直观的方式对日常工作和其他活动做一个概述。您可以利用这种对日常工作的概述，制定一个检查清单，列出一天中的一些时刻，在此可以建立一个基准线，随后检查安全指标。

在这个练习中，我们会建议您用绘画的方式将日常工作呈现出来。虽然画画可能看起来有点奇怪，但这是一种有用的方式，可以帮助您从不同的角度来看待您 通常不会从安全角度考虑的活动。

画成什么样都没关系，您自己能看懂就行。

画一个典型的工作日，或者画一个您认为敏感危险的活动的特殊日子。只需从您早上醒来时的位置开始，并考虑以下事项：

1. 吃早餐的时候您在哪

1. 您如何到达办公室？乘坐什么车，与谁一起，通过哪些区域？

1. 当您上班时会带什么电子设备？还携带哪些其他东西（钥匙、门禁卡、皮夹…）？

1. 您在哪里工作，还有谁？您如何工作，以及使用什么设备？

1. 如果您在工作期间吃午餐或晚餐，请将其包括在内。您给自己多长时间以及在哪里吃饭？

1. 您什么时候停止工作？如果您不在家工作，您如何回家？走哪条路？

1. 您通常几点睡觉？睡前做什么？

1. 除了工作和家庭，您经常在哪里度过业余时间？

当您绘制出一天的快照后，开始试着寻找您的 “基准线”，即 正常的一天看起来像什么，以便以后检查您的物理环境中是否有任何不寻常的迹象发生。

一些建议可能包括：

- 您驾驶的车辆：是否有任何被动过的迹象（车轮、刹车、方向盘等）？

- 您上班的路线：这些区域中是否有危险？是否值得检查一下是否存在被跟踪？

- 您的办公室或工作区：到达时和离开前，一切东西都在适当的位置吗？门窗是否锁好？

- 紧挨着您的住所或办公室的空间：是否有陌生人、警察、或陌生的车辆出现？

（更多现实中反侦查的技巧详见本板块S05）

🔑

如果您检查到周围环境存在危险信号，记下您的观察和那个时刻，并考虑与值得信赖的朋友、邻居和同事分享。如果您认为自己的风险很高，可能需要和您的家庭成员或其他亲密朋友分享您的观察，让他们有所准备 —— 告诉他们万一出事应该怎么做。

根据结果创建一个检查清单：您将检查什么，何时检查？

备注与技巧

经历这一过程是为了帮助确定您根据自己的判断感觉应该采取行动或采取预防措施的情况，以及注意到您可能感到需要更加小心的时刻。如果您在反抗行动中开展了许多不同的活动，请尝试针对您工作的不同方面重复这一练习。

与值得信赖的朋友或同事分享这些信息的目的是为了确保您仔细检查和确认您的观察结果和/或涵盖您可能忽略的潜在领域。

⚠️

重要提示：在比较危险的活动中，如抗议行动或抵抗运动，或监测和记录任务，您必须特别注意安全指标，特别是考虑到周围的情况可能会迅速变化。

考虑针对这些特定的活动进行这项练习，并记录下任何不寻常的时刻，在这些时刻，您应该确保检查您的物理环境中可能存在的任何危险迹象。列一个清单。

[image]
[image]

S01E05-T1 制定检查清单

[image] 关键词	个人 团队 基准线 威胁识别
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025/03/07
[image] **Description**	练习

[image]
[image]

S01E05-T4 态势监测和威胁清单

[image] 关键词	威胁模型 态势监测 时局
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025年3月7日
[image] Description	练习

[image]

单独做或和您的团队一起练习都可以。请考虑以下问题：

1. 您目前如何进行态势监测和分析？您和队友们目前有哪些空间可以讨论社会的持续发展这类议题吗？尤其是与你们的共同利益密切相关的发展；

1. 您对此有何信息来源？ —— 列出这些内容，并针对它们提供的信息质量，分别记录它们的优缺点。这些信息源是客观的还是有偏见的？

1. 考虑一下过去12个月在本地、本国和国际范围内发生的事，并列出5 ~ 10个您认为重要的动态。您可能不需要对它们进行分类，但是请务必考虑：政治发展、经济发展、社会发展、技术发展、法律发展、环境发展；

1. 这些发展是否会直接或间接影响您的安全性？如果是，可以怎么办？去年您有遭受任何袭击或事故吗？它们与这些发展有何关系？

注：如果您对过去的12个月中没有想到新的发展，请考虑一般的显著特征。

处于危险中的人权维护者通常会收到来自其对手的公然威胁，例如来自个人、团体或组织的信息，公开表示要对您造成伤害。

这些威胁的意图是迫使您停止手头正在进行的工作 (至少是暂时停止)、惩罚或伤害您，进而杀鸡儆猴以阻止其他人。

这种信息构成了一种特殊的威胁指标，因为它们已经对您产生了心理影响，很可能是实际威胁的前兆。

一般来说，"公然的威胁" 是故意的 (它们有明确的意图)、战略性的 (它们是阻碍您工作的计划的一部分)、个人化的 (它们是专门针对您和您的队友的)和基于恐惧的 (它们是为了吓唬您，让您放弃反抗)。

公然威胁也可能在您的对手在公开声明中或通过司法骚扰或拟议的立法进行或暗示。比如，中国的 "社会信用评分"，在它刚刚提出时（2015年）我们强调过它是一种公然威胁。

这种威胁非常有效，也很 "经济"，因为它们可以在不进行实际威胁的情况下达到目的。

☉

必须牢记，虽然一些已经发生的公然威胁可能会产生具体影响，但另一些威胁则是为了制造新的无端恐惧，而没有计划采取实际行动进行伤害。您需要清楚地分辨它们。

在分析公然威胁时，回到您从前制作的行为者图谱中，考虑有关对手的资源和利益，以了解是否构成了真正的威胁。

在研究了您所面临的威胁并考虑了它们所带来的风险（基于可能性和

影响）之后，下一步就是建立一个优先级排序的威胁清单，并详细分析每一种威胁的性质：它们的原因、影响和来源，以及所需的资源、现有的行动和您可以采取的下一步措施。这项活动将为您建立战略打下基础，以降低威胁发生的可能性，并在威胁发生时降低其影响。

此练习将帮助您确定威胁的优先级，并查明原因、后果、来源以及所需的资源、现有措施和可能的后续步骤。

您需要准备：

- 行为者和关系图谱（您在上一集的练习中制作的那个东西）
- 信息生态系统（您在前面的练习中分析的东西）
- 安全指标（本集最初时您分析的东西）
- 影响或发生的可能性
- 纸笔、挂图、标记物（便签、马克笔…）

首先，从上一次练习的集思广益开始，考虑所列出的威胁的可能性和影响。选择您认为最有可能发生的和影响最大的威胁作为案例，用于下一次练习。

根据特定活动区分并组织这些信息，可能会很有用（例如，将在抗议活动中具体出现的威胁与您的团队日常的运行中有关的威胁区分开）。

首先，基于影响/可能性的矩阵，并使用提供的示例模板，仔细分析您认为应该是最高优先级的威胁。

写下威胁的标题和摘要。

对于每个威胁，如果它是一个复杂的威胁，您可能会决定划分出子威胁，并分析它们 —— 例如，如果将办公室被警方突袭与人员被逮捕两个威胁分开，以涵盖每个威胁将包括的众多后果 —— 潜在的逮捕、没收设备、司法骚扰等，可能更容易分析。使用更多的行来展开每个子威胁中的以下各项。

针对每一种威胁，研究以下问题。可能有些威胁比较复杂，有些答案需要单独的空间。建议根据需要尽可能多地使用行。例如，如果一种威胁构成对一个人的攻击、同时遭受攻击的还有他们所携带的信息 —— 持有真相的公民调查人士经常会面对这样的威胁，您可能想用单独一行来描述信息方面，用另一行来描述有关的人。

WHAT：描述如果威胁被实施会发生什么。想想它对您、您的组织、您的盟友可能产生的影响。包括对物理空间的破坏、对人的压力和创伤、信息泄露等等。尽可能想到全面，这样您才能提早准备PlanB应对方案。

WHO：确定威胁背后的个人/组织/实体。参照您前面构建的行动者图谱，您可以把重点放在有关这个特定对手的信息上。

- 这些对手的能力是什么？
- 他们在实施这些威胁方面会有什么限制？（他们的能力极限是什么？）
- 是否有中立方或盟友可以影响他们？（您有可能的帮手吗？）
- 是否有针对您或盟友实施此类威胁的历史？（如果有，研究整件事，您可以从这里得出什么经验教训吗？如果那种事重新发生在您身上，提前思考和准备有助于您比前车之鉴做得更好）

WHOM/WHAT：查明威胁的潜在目标；被窃取的具体信息、受到攻击的具体人员（身体、情感、经济等方面的攻击全包括）、受到威胁的财务和资源（被没收的设备或被破坏的财产）；

HOW：这是关于分析您的对手，他们想要什么信息？对手进行威胁所需的信息是什么？他们可以从哪里获得这些信息？

举例：只有当对手对攻击目标有足够了解的情况下，他们才能够实施最严重的攻击。想想看，他们可以从什么地方了解您？社交媒体、网络文章、动员海报、您身边的毫无戒心的熟人、对您的跟踪侦查、他们所掌握的关于您的历史档案 …… 这其中哪些东西是您可以减少被他们了解的？通过删除和篡改信息以迷惑您的对手，您知道该怎么做吗？

尤其是在您不得不逃离此处的时候，您需要清楚地知道HOW这个问题的答案。

再比如，您的对手正在准备对您采取恶意软件攻击，他们有可能掌握什么样的恶意软件？其目标最有可能是导致您工作的系统崩溃、还是对您的组织中关键人员进行秘密监视？或者破坏您的调查中能揭露您的对手的罪证？…… 他们将最有可能如何制定这一攻击方案？以什么为突破口？您和组织的薄弱环节在哪？如何阻止对手获得攻击突破口？

WHERE：描述潜在攻击可能发生的地方。攻击者是否需要像物理攻击中经常出现的那样进入您所在的区域？相关地点有什么特点？您如何才能保证安全？它的哪些地方相对更危险？

举例：就如我们在反情报相关内容中经常指出的那样，专业的攻击者会避免进入目标人的地盘，因为那是目标人所熟悉的，而攻击者不够熟悉的；相反，他们会努力把目标人引入他们的地盘。所以，您需要真的对自己的地盘非常熟悉，哪里是通道、哪里是掩体、哪里可以获得临时的武器、哪里地形复杂可以甩掉攻击者 …… 这就是我们在“超强记忆力” 中所强调的部分之一。

阐述与这一威胁有关的心理、情感和健康因素，包括您的压力水平、疲劳、恐惧和其他因素；对这一威胁可能发生的影响，考虑以下问题：

1. 您当前的心态会如何影响正在执行的计划和应急措施？

1. 这种威胁是否发生在特定的活动中？在这种活动中，您发现自己处于什么样的精神或身体状态？有哪些最佳做法可以保护您，或者哪些做法可能使您更容易受到伤害？

1. 您的行为或心态的哪些要素实际上可能会增加发生这种情况或其影响的可能性？

如果您希望以书面形式记录练习的结果，可以使用以下格式：

[image]

一旦您进行了这些分析，下一步就是审视自己，考虑您现有的做法、资源和其他能力，如何能够保护您免受危害，以及您在做法和资源方面尚且存在的缺陷、以及其他弱点如何使您容易受到其影响。

我们将在下一集的战略分析中详细解释更深入的做法。

[image]
[image]

S01E05-T2监测自己的压力水平

[image] 关键词	压力监测 心理安全 自测
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025/03/08
[image] **Description**	练习

[image]
[image]

S01E05-T3 确认可能遭受的所有威胁

[image] 关键词	判断力 威胁模型
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025/03/09
[image] **Description**	练习

[image]
[image]

S01E05-T4 态势监测和威胁清单

[image] 关键词	威胁模型 态势监测 时局
[image] 关联	[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全 S01E05 - 紧贴时局
[image] 创建时间	2025/03/10
[image] **Description**	练习

[image]
[image]

S01E06-T1 剖析每一种威胁

[image] 关键词	威胁识别 心理安全
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全 S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025/03/11
[image] **Description**	练习

[image]
[image]

S01E06-T2 找到弱点建设新的防御能力

[image] 关键词	心理安全 脆弱性 防御
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全 S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025/03/12
[image] **Description**	练习

[image]
[image]

S01E06-T3 审核防御能力

[image] 关键词	自检 防御
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025/03/13
[image] **Description**	练习

[image]
[image]

S01E06-T3 审核防御能力

[image] 关键词	自检 防御
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全 S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025年3月14日
[image] **Description**	练习

在本练习中，您可以进一步发展您所确定的提高安全的必要新能力。从接受、威慑和保护战略的角度来考虑这些能力，将有助于您了解自己的总体安全战略，并帮助您想出更多的策略以进行发展。

如果您想写下练习的结果，可以考虑使用下面这样的格式：

[image]

步骤1：查看您在上一练习中确定的＜准备新构建的能力＞。考虑它们是否是：

- 一个有效的招数？
- 威慑战术？
- 护身符？
- 还是上述各项的结合

步骤2：现在，针对每种威胁，考虑可以采用的其他新策略，以便：

- 提高对手或社会对您的工作的容忍度和接受度
- 通过提高攻击成本来阻止对手对您采取行动
- 保护自己免受威胁，并更有效地应对威胁

继续使用您提出的新想法来扩展这个新能力的列表。

步骤3：对于已确定的每种新能力，请考虑您将需要使用的资源（财务和物质）以建立这些能力。

[image]
[image]

S01E08-T1 大家怎么看

[image] 关键词	团队 自检
[image] 关联	[image]安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动
[image] 创建时间	2025/03/14
[image] **Description**	练习

[image]
[image]

S01E06-T1 剖析每一种威胁

[image] 关键词	威胁识别 心理安全
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全 S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025年3月14日
[image] **Description**	练习

[image]

在此练习中，您可以根据自己现有的安全实践和与之相关的其他能力，考虑您在前面内容中确定并认为最重要的每一种威胁。这将为您提供一个 “基准线”，您可以在此基础上进行建设和改进。

对于您所确定的每一种威胁，都有一系列的问题。在这里，您可以将您现有的安全做法和能力与这些问题中的每一个问题联系起来，具体如下：

谁/或什么会受到威胁？ —— 在此确定有哪些能力（如果有的话）已经在保护此人或此物免受威胁。＜能力＞ 的例子可以包括，比如：

- 在司法骚扰案件中：您具有良好的法律知识，或者您确认有非常可靠的朋友可以帮您做到这点；
- 在被没收电脑的情况下：您有加密的硬盘、隐藏的加密分区设置妥当……

威胁的背后操手是谁？—— 您是否已经有某种策略来与这个行为者接触？您是否有任何策略或资源可以阻止他们对您采取行动？如果有，是什么？如果他们以前曾对您采取过行动，您是否以某种方式做出了回应？如果有，如何回应的？如果没有，也没关系：这在帮助您找出差距时很重要。

【举例】如果您的对手是政府间谍，他们正在试图从您和队友的私密交流中挖掘能把你们连锅端的情报线索，那么您能阻止他们成功的策略就是加密、隐写术、加密卷等技术；您的资源是对技术的熟练掌握和队友之间的密切合作；想想看您有没有曾经遭遇过类似的事？还是您听说其他人经历过？其中有哪些经验教训能帮您在下一次做得更好？…… 总结它们。

攻击者会怎么做？—— 他们需要哪些信息来进行攻击？您是否采取了任何信息保护措施或反监视做法，以防止这些信息落入攻击者手中？

【举例】如上面例子，攻击者首先要知道您和队友的真实身份，才能对你们采取行动。如果您是活动家，是站在前台的人，您可能难以采取假名身份，但您的队友是行动者，成败更多取决于他们。于是，如果您的队友采取的假身份，那么即便攻击者的入侵拿到了你们的私密对话，他们也不知道行动者的真实身份，就无法做到在行动之前扼杀它。您所要做的就是，避免让攻击者了解到与您合作的人的真实身份。您的组织中应该对此做好安全培训（推荐采取本站的培训框架，您可以对其进一步的本地化处理）。

在哪里？ —— 攻击者需要怎样接近您或进入您的财产？您如何保护自己周围的物理空间（如 建筑物、车辆、电子设备、私人物品等）？例如，在危险的环境中，您有哪些 “常识性” 的做法可以保障自己的人身安全？

【举例】一些中国朋友曾经讲述过一个在警察敲门前的 “终极做法”，即 准备一堆强磁铁，将电脑和磁铁包在一起，塞到妥当的地方。这就是常识性的做法。但无法保证这样做能完全避免取证软件，反而会显得您 “很可疑”，警察会因此脑补出很多秘密。

心理、情感和健康策略 —— 包括为应对这一威胁而采取的任何做

法：您是否有任何有助于减轻压力、疲惫等心理威胁的做法、并提高可能有助于应对这一威胁的心态和意识？

如前文所述，只有当您能保持精力和敏锐度的时候，才更容易发现并有效应对威胁带来的挑战。

在可能的情况下，试着考虑这些方面相对于您所确定的每一个威胁。如果您想不出一个或多个问题的答案，那也没关系：这意味着您发现了一个有待填补的缺口。

您将在后面的练习中考虑这些差距，并利用这些差距来确定您需要哪些新的资源和做法。

备注和技巧 ——

请注意：对于您给出的每一个答案，都要考虑这种做法或能力是否积极。您是如何知道的？如果您错误地认为现有的做法可以保护您的安全，就会有一种制造虚假安全感的危险。

如果您对某件事情不确定，不妨花点时间好好想一想，和您的同事或值得信赖的朋友谈谈，以便获得新的看法。

[image]
[image]

S01E06-T2 找到弱点建设新的防御能力

[image] 关键词	心理安全 脆弱性 防御
[image] 关联	[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全 S01E06 - 开发您的能力，缓解您的脆弱性
[image] 创建时间	2025年3月14日
[image] **Description**	练习

[image]

在本练习中，您可以根据您现有的安全实践中的差距和您的弱点，考虑您在前面练习中确定并优先考虑的每一种威胁。这将使您更清楚地了解自己需要在哪些方面开始建设新的能力。

准备好笔和纸或其他书写材料。

再一次，使用您在前文练习中确定的威胁列表，以及在上面练习中确定的现有能力和做法。

在这里，您可以尝试确定自己现有实践中的差距和您的弱点，与您之前回答的每个问题相关。

请考虑以下问题：

谁/或什么受到威胁？—— 在此确定存在哪些差距或弱点（如果有的话）会使这个人或事物更容易受到威胁。

【举例】脆弱性可能包括：

- 在遭遇司法骚扰的情况下，一个人没有多少法律知识
- 在被没收电脑的情况下，没有密码的硬盘，或没有加密

谁是威胁的幕后黑手？ —— 也就是您的对手是谁？您在影响这个行为者的能力方面存在哪些弱点或差距？例如，如果没有办法直接与这个对手接触，使其接受您的工作、或阻止他们发起攻击，这可以被认为是一个差距。

这些威胁行为者会怎么做？—— 他们进行攻击所需的信息是什么？您在处理与自己的工作有关的信息的方式上是否有任何漏洞可能会助长这种威胁或使其更具破坏性？

漏洞在哪里 —— 您周围的物理空间（如建筑物、车辆、电子设备、私人财产等）的哪些方面使这种威胁更有可能发生或更具破坏性？例如，在办公室遭到警方突袭和被盗窃的情况下，门锁不牢固就是一个弱点。

心理、情感和健康方面的考虑 —— 在这一威胁的背景下，压力、疲劳等会对您产生什么影响？在您的健康实践中存在哪些差距或弱点，可能使这一威胁更有可能发生或更具破坏性？就如疲劳驾驶容易翻车，一样的道理。您需要对自己有清楚的了解，基于您通过前面章节中的练习得出的答案。

尽可能改善您找到的一切弱点。

在接下来的内容中我们将探索有关如何在整体安全策略中开发和实施新能力的动力。

定义一个全面的安全战略与简单地采取临时或即兴的方法来保护安全，有很大的不同。您对威胁的许多本能反应或临时性安全协议，也许能保证您的安全，但其中一些不一定有效，甚至还可能是有害的。

现在，您已经开始通过前面练习中确认的新战术和能力来更新您的安全战略。这些应与维持和扩大您作为人权维护者工作的社会政治“空间”的总体战略有关；这一概念将在下文中阐述。

示例

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

[image]
[image]

S01E08-T1 大家怎么看

[image] 关键词	团队 自检
[image] 关联	[image]安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动
[image] 创建时间	2025年4月3日
[image] **Description**	练习

[image]

这是一项基本练习，它可以帮助您检查组织成员对组织安全措施实施的看法。

您可能希望关注组织的整体安全绩效，或者组织安全实践的一个更具体的方面，如数字安全、心理健康、旅行安全、冲突地区的安全等。

第1步：简单画一个圆圈，将其分为8个不同大小的部分，每个部分都有一个标题，这就是您自己的 “安全轮”。

第2步：分配给轮盘上的每一个部分就按照您认为恰当的比例，然后分别给它们涂上颜色，以反映组织实施最佳实践的程度 —— 这些颜色代表什么，您和队友应该有共识。

第3步：对于每一段，每个人都应该分别找出目前阻碍自己或整个组织更好地遵守最佳实践的障碍。

第4步：同样，考虑每个障碍或问题的潜在解决方案是什么。

第5步：比较组织成员之间填写的结果。哪些地方有共识，哪些地方有分歧？分析一下，为什么会出现这种情况？

第6步：和您的队友一起尝试确定必须优先改进的领域。

在评估您的组织目前的情况时，您将很容易发现需要改进的领域。这些都应成为更新和扩大您的安全计划和协议的基础。

这个过程应该可以实现：

- 在实施新的最佳做法方面有一个明确的目标 —— 您的所有计划将尽可能接近或符合这一目标；
- 包括一个时间表，说明谁需要参与，何时参与、以及对他们的期望；
- 明确规定每项改进所需的资源。

[image]
[image]

组办安全议题研讨会 S00-T1：为自己定义安全

[image] 关键词	互助 团队 心理安全 研讨会 组织
[image] 创建时间	2025年6月1日
[image] **Description**	练习

[image]

[image]

建设中！敬请期待。

[image]
🔥

反渗透/线人&减轻背叛的损失-AntiInfiltration&informant

不幸的是，与寻常的理解完全相反 —— 被镇压系统瞄准事实上是一种巨大的失败，绝非“成功”； 如果必需衡量“价值”的话，我们每个人都应该致力于对我们自己的战略、对我们自己的战友和政治理想“具有越来越大的价值”，而不是对敌方的维稳指标有价值！这两种价值恰恰相对立。 也建议您警惕那些喜欢吹嘘自己的“敏感级别”或过往功绩的人，这至少意味着此人要么并不了解前线的生存策略和价值判断，要么，可能是在钓鱼。

[image]
[image]

安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

[image] 关键词	原则 团队 安全文化 整体 预防性
[image] 关联	[image]安全文化和广阔的生活；[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病；[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09
[image] 创建时间	2025年1月1日 10:00 (GMT+8)
[image] Description	心理安全；行动安全性；反渗透和协作

我们从来没有告诉过您这些东西，也永远不会告诉您。感谢您记得这点。

- Table of Contents

1、所有安全文化的核心原则 —— 也是再怎么强调也不为过的一点 —— 就是：人们永远不应该知道任何他们不需要知道的敏感信息。
2、不要问，不要说。
3、您可以随时对任何人说不，关于任何事。
4、千万不要把您的朋友交给敌人！
5、不要让敌人太容易弄清楚您的目的。
6、不要在公开场合抛出任何您认为自己可能会在某个时候想尝试的直接行动想法！
7、制定一个在公开场合与战友沟通的私密通信。
8、制定方法，确定一个团体或情境的安全级别。
9、开会地点是安全的一个重要因素。
10、要意识到您身边的人是否可靠，特别是可能与您合

作进行地下活动的人。
11、不要过于分心担心别人是否是线人，如果您的安全措施有效，渗透就应该根本不重要！
12、学习并遵守与您交往的每一个人的安全期望，尊重风格的差异。
13、在安全方面，要让别人清楚地知道您的需求是什么。
14、为别人着想。
15、安全文化是一种礼仪，是避免不必要的误解和潜在的灾难性冲突的方法。
16、安全文化不是偏执狂的制度化，而是提前将风险降到最低，避免不健康的偏执狂。
17、不要让猜疑被用来对付你。
18、不要被虚张声势所吓倒。
19、时刻准备着您被监视的可能性，但不要误以为吸引了监视就等于行动有效！
20、“沉默”不是无声。
21、在躲避敌人侦查的需要和潜在朋友接触的需要之间进行平衡。
22、当您计划一项行动时，首先要确定与之相适应的安全级别，并从那里开始采取相应的行动。
下面是一个可能的安全等级评定系统的例子，从窄到宽：
并且，根据您所需的安全级别选择将使用的通信方式同样非常重要。下面是与上面概述的系统相对应的不同级别的通信安全性的示例 —— 要对应着看哦：

[image]

安全文化是敏感人士社区共享的一套习俗。我们称为前线社区。其成员很可能会成为政府的目标，而安全文化的目的就是帮助您将风险降到最低。

有了安全文化后，每个人都不用再从头开始反复制定安全措施了，而且可以帮助抵消压力情况下的偏执和恐慌—— 当然，也能帮助您远离监狱。 BACK [image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性

[image]

安全文化和安全协议是不同的；

协议和文化的区别在于，文化会变成无意识的、本能的，从而毫不费力；

一旦最安全的行为已经成为您的集体中每个人的基本习惯，您就可以不需要再花更多时间和精力去强调它的必要性、或者承受没有它的后果、或者担心自己有多大的危险了，

因为您会知道自己已经在尽一切努力去小心。

如果您养成了不泄露自己任何敏感信息的习惯，您就可以放心地和陌生人合作，而不必为他们是否是政府线人而苦恼；如果每个人都知道在电话里不能说什么，您的敌人就算尽情地窃听电话线也不会让他们有任何收获。

[image]

在本站“反渗透”专题中查看相关具体建议。

直接行动准备工作请从“威胁知识库”相关主题开始：🐱渗透者 □告密者（线人）

以下有22条内容，是您应该最基本做到的。

[image]

1、所有安全文化的核心原则 —— 也是再怎么强调也不为过的一点 —— 就是：人们永远不应该知道任何他们不需要知道的敏感信息。

这是一个重要原则。即：

[image]

直接行动准备工作从这里开始：[image]信息最小化原则

知道一些可能危及个人或项目的信息的人越多，风险就越高 —— 无论这些信息是犯有非法行为的人的身份、私人会议的地点，还是未来活动的计划 —— 就越有可能使这些信息落入坏人手中。

与不需要这些信息的人分享这些信息，对他们来说是一种伤害，同时也是对那些处于危险中的人的伤害：因为这会将他们置于一个不舒服的境地，即 只要一个错误的举动就能搞砸别人的生活。例如，如果他们被审问时，他们就会有一些东西需要隐瞒，就会有压力，不是所有人都擅长处理压力的。

2、不要问，不要说。

不要要求他人分享您不需要知道的机密信息。不要吹嘘您或他人做过的任何敏感的活动，也不要提及将要发生或可能发生的事，甚至不要提及其他人对参与此类活动的兴趣。

无论何时说话都要保持清醒，不要让偶然的暗示不经意地掉出来。

3、您可以随时对任何人说不，关于任何事。

不要回答任何您不想回答的问题—— 不仅仅是对警察，也包括对其他活动家，甚至是您的亲密的朋友，都是如此：如果有什么您觉得不安全的事，就不要分享。

这也意味着对别人不回答问题的现象不要感觉不舒服：如果有一个对话他们想保留给自己，或者他们要求您不要参加一个会议或项目，您不应该把这当作针对您个人的问题 —— 他们可以自由地这样做是为了大家都好。

[image]

信任分级应该是一个公认的原则。

同样，不要参加任何您觉得不好的项目，也不要和任何您觉得不放心的人合作，不要在任何情况下忽略自己的直觉，如果出了问题，惹了麻烦，您也不想有任何遗憾。您有责任不让任何人劝您去冒您还没准备好的风险。

4、千万不要把您的朋友交给敌人！

如果被抓了，永远，永远不要交出任何可能危及他人的信息。

有些人建议直接行动小组的所有参与者都要进行明确的宣誓：这样一来，在最坏的情况下，当压力可能会使您很难区分放弃一些无害的细节和完全出卖自己之间的区别的时候，每个人都会清楚地知道他们已经对彼此做出了什么承诺。

5、不要让敌人太容易弄清楚您的目的。

在您所采用的方法，或您所选择的目标，或你们见面讨论事情的时间和地点上，永远不要太容易被预测到。

在您进行最严肃的直接行动的斗争中，不要在公开方面太显眼：不要让您的名字出现在邮寄名单上，也不要出现在媒体上，有些情况下也许要完全避免与公开的组织和运动的联系。

[image]

如果您和几个队友一起参与了真正严肃的秘密活动，您可能要限制你们在公开场合的交往，甚至应该完全避免让自己看起来认识对方。

政府间谍可以很容易地获得从您的手机中拨出的电话号码，并会利用这样的名单建立个人之间的联系网络；从您的电子邮件，到您从图书馆借阅的书籍，特别是社交网站，都是如此。

看一个示例：https://iyouport.substack.com/p/9db?utm_source=publication-search

不要留下任何蛛丝马迹：信用卡的使用、加油卡、手机通话等都会留下您的动静、购买历史记录和联系人关系网络的记录。如果您需要的话，要准确一个掩饰性的故事以解释为什么会产生相关“联系”，并需有可证实的事实支持这个故事。

[image]

相关主题见：[image]匿名购买 ；分身 ；[image]假身份 ；[image]关系网络图谱

在 **[image] S04完美隐身-总章节：机智是重要实力** 中看到具体做法。这里的链接是该系列内容的最后一集，其中包含完整列表。

小心您丢掉的垃圾！可能会暴露您的身份—— 并非只有辍学者才会去扔垃圾，垃圾箱潜水是社交工程师的专长之一。对您的每一份书面文件和复印件都要仔细权衡，用您的对手的眼光去权衡它们与您的安全的利害关系—— 把它们都放在一个地方，这样您就不会不小心忘掉一个，一旦不再需要它们，就把它们彻底销毁。

您需要能做到这些敏感证据的数量越少越好，要习惯使用自己的记忆力。

确保在您书写的表面上没有留下任何这种书写的印记，不管是木制的桌子还是纸垫。要知道每次使用电脑也会留下痕迹，尤其是要知道该怎么处理痕迹。在**S03**中看到详细解决方案 BACK **[image] S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人**

[image]

6、不要在公开场合抛出任何您认为自己可能会在某个时候想尝试的直接行动想法！

等到您能真正召集到一群您认为都会有兴趣尝试的人时，再提出一个想法；例外的是您的亲密伴侣，您要和她/他一起进行头脑风暴，并提前商量好细节 —— 当然是在安全的情况下，在您的家门外，远离你们的工作单位。

[image]

相关自卫措施：[image]户外无设备对话

在您认为时机成熟之前，不要提出您的想法。

只邀请那些您非常确定会加入的人 —— 您邀请的每一个人如果最终没有参加，就会带来不必要的安全风险，如果他们觉得您提议的活动愚蠢得可笑或在道德上是错误的，那就更麻烦了。

只邀请能够保守秘密的人 —— 这一点对他们是否决定参加至关重要。

7、制定一个在公开场合与战友沟通的私密通信。

在公共场合，比如在被召集讨论可能的直接行动的会议上，要想办法与您信任的队友暗中交流安全问题和舒适度，这一点很重要。

[image]

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

知道如何在别人看不出你们在来回发信息的情况下衡量对方的感受，将使您省去试图猜测对方对某一情况或个人的想法的困惑，并且帮助您避免在事情发生时不能把朋友拉到一边；也不会显得奇怪。

当您召集一个更大的团队提出行动计划时，您和您的亲密队友也应该清楚彼此的意图、冒险的意愿、承诺的程度、和对他人的看法，以节省时间，避免不必要的歧义。

如果您以前没有参加过直接的行动计划圈，您会惊讶于即使大家都做好了准备，事情会同样会变得多么复杂和曲折。

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

8、制定方法，确定一个团体或情境的安全级别。

在一次规模较大的会议开始时，如果不是每个人都认识，您可以进行一个快速的程序，那就是 “担保” 游戏：当每个人自我介绍时，所有能担保此人的人都举手。

请注意，您应该只为您有信心和值得您信任的人担保。希望每个人都通过链条上的某个环节与其他人联系在一起，无论怎样，至少大家都知道事情的现状。

[image]

一个明白良好安全的重要性的活动家，在这种情况下，如果没有人在场可以为他担保，其他人可以请他离开，如果他理解安全文化是什么，他就不应该会觉得受到了侮辱。

9、开会地点是安全的一个重要因素。

您应该选择一个完全没有监视的地方(不要选私人住宅！因为地点会与房主的身份联系在一起，将很容易曝光你们的关系网络)；您不应该选一个可以被全部观察到的地方 (比如，不应该是第二天行动地点对面的公园)；不应该选择一个可以看到您进出的地方，或者有人可能会突然进入的地方—— 这里要使用您派遣的侦察员。会议开始后要锁门，注意任何可疑的东西。

[image]

相关自卫措施：[image]监控侦测 ；[image]藏匿点或安全屋 ；[image]突袭应对措施 ；[image]户外无设备对话

小团体可以通过散步聊天；大团体可以在安静的户外环境 —— 如果有时间的话，可以去登山或露营，也可以在公共建筑的私密房间里见面，比如图书馆自习室或空的教室。

[image]

最好的情况是：虽然不知道你参与了直接行动，但你和镇子对面开咖啡馆的老板关系很好，他不介意在某个下午把后面的房间让给你开个私人派对，而不问任何问题。

[image]

10、要意识到您身边的人是否可靠，特别是可能与您合作进行地下活动的人。

意识到您认识这些人多久了，他们在您的社区中的参与和他们在社区外的生活可以追溯到什么时候，以及其他人与他们的关系经历。

[image]

相关自卫措施：[image]关系网络图谱

与您一起长大的朋友，如果你的生活中还有他们，可能是直接行动的最佳伙伴，因为您熟悉他们的长处和短处，以及他们处理压力的方式 —— 当然，您也知道他们就是他们所说的人。

确保只把您的安全和项目的安全性托付给头脑清醒的人，他们有着与您同样的优先级和承诺，而且没有什么需要去证明的。

从长远来看，要努力建立一个由具有长期友谊和共同行动经验的人组成的社区，并与其他此类社区建立联系。

11、不要过于分心担心别人是否是线人，如果您的安全措施有效，渗透就应该根本不重要！

不要浪费您的精力让自己变得偏执而不善于交际，并不需要怀疑您遇到的每一个人—— 这点我们在 S01中有过专门介绍 [image]抗议中谨防常见危险：整体安全 S01E11 - 协作和互助就是战斗力

如果您把所有的敏感信息都保存在 仅限绝对必要的队友 的圈子里，只和那些可靠的、有经验的、您能核实其历史的朋友合作，加上绝不泄露任何有关您私人活动的信息，那么特工和警察的线人就无力收集证据来对付你。

[image]

一个好的安全文化，应该让这些害群之马是否在您的社区里活动都能在实际上已经无关紧要。重要的不是一个人是否与警察有牵连，而是他是否构成实际安全隐患；如果他被认为是不安全的（双重含义），就绝对不应该允许他去决定其他人的安全性。

12、学习并遵守与您交往的每一个人的安全期望，尊重风格的差异。

要与他人合作，您必须确保他们对您有宾至如归的感觉；即使您不与他们合作，您也不应该让他们感到不舒服，或者无视他们比您更了解的危险。

当涉及到计划直接行动时，如果不遵守特定社区所接受的安全文化，不仅会破坏您与他人合作的机会，而且会破坏项目发生的可能性——例如，如果您提出一个他人计划在他们认为不安全的环境中尝试的想法，他们可能会被迫放弃这个计划，因为它现在可能与他们有关。

在您提出直接行动的话题之前，请大家为您勾勒出他们具体的安全需求。

[image]

返回 - 相关练习：[image]S01E08-T1 大家怎么看

13、在安全方面，要让别人清楚地知道您的需求是什么。

遵守他人期望的必然结果是，您必须让他人容易遵守您的期望。

在任何关系的开始，您的私人政治生活经历可能会成为一个问题，强调您的活动有一些细节需要保密。这可以让您在已经足够紧张的情况下省去很多戏剧性的事。您会懂的。

[image]

这并不是关于信任问题，而是主体性问题 —— 敏感的信息从来不是、也永远都不会是可交换交易的东西。

14、为别人着想。

向身边的人明确说明您的存在可能会给他们带来哪些风险。或者您已经计划好的行动，至少在不违反其他安全文化戒律的情况下，您能做到什么。

让周围人知道在您的能力范围内，您自己要承担哪些风险：例如，您是否能承受被逮捕的风险（如果有未完成的逮捕令，如果您是一个“无证移民”，等等），您要承担哪些责任，您是否有任何所谓的敏感点让当局可以抓到“把柄”。

我们所有人都不该因为彼此的吹嘘隐瞒而陷入困境。诚实是互爱的力量。

如果别人在您点燃火堆的地方丢了一条横幅，警察可能会以纵火罪起诉他们；即使罪名最终不成立，您也不想发生这种麻烦的。或者您堆

砌的路障不小心堵住了其他人计划中的逃生路线。这类把球踢进自家门里的失误都不该发生。

[image]

如果您帮助发起了一场突破受允许区域的突围游行，尽量确保您的身体挡在警察和其他已经赶来但不一定了解其中风险的人之间；如果您推动了行动的升级，请确保当警察出现时，其他对此毫无准备的人不至于还站在这里迷茫。

勇气源于理性的抉择和妥善的计划。无论您从事哪种风险项目，一定要做好准备，要聪明地去做，这样就不会有其他人在您犯错的时候，去冒着意想不到的风险帮您。

15、安全文化是一种礼仪，是避免不必要的误解和潜在的灾难性冲突的方法。

安全问题永远不应该成为让别人感到被排斥或自卑的借口 —— 虽然要避免这种情况可能需要一些技巧！—— 就像任何人都不应该觉得自己“有权”参与到任何别人希望保密的事情中去。

[image]

对于那些违反社区安全文化的人，第一次不应该受到太严厉的斥责—— 这不是一个够不够时髦、够不够积极的礼节，也不是一个够不够融入的问题，而是建立群体期望，温和地帮助人们理解其重要性的问题。

人们被迫启动防御状态的时候，就是他们最抵制建设性批评的时候。不要促成那样的状态。

尽管如此，对于犯错的队友，您始终 应该立刻告知 他们是如何让别人处于危险之中的，以及如果他们继续这样做会有什么后果。

对于那些不能理解这一点的人，必须巧妙而有效地将他们拒之于所有

敏感情况之外。

[image]

16、安全文化不是偏执狂的制度化，而是提前将风险降到最低，避免不健康的偏执狂。

如果花更多的精力去担心自己受到了多少监控渗透，而不是有用的减少监控渗透带来的危险，就像不断猜测自己的防范措施、不停怀疑队友的草木皆兵那样，是完全消耗精力的，适得其反的。

[image]

良好的安全文化应该让大家都感到更多轻松、更多自信，而不是减少。同时，如果指责那些遵守比你们更严格的安全措施的人或团队是“偏执狂”，同样是没意义的！

—— 要记住，我们的敌人始终是要对付我们所有人的。我们除了保护彼此，别无他法。

17、不要让猜疑被用来对付你。

如果敌人不论如何都无法得知你们的秘密，他们还有最后一招，那就是：让你们反目成仇，自掐出最核心的秘密来。

渗透者可以散布谣言或四处指控，在团体内部或团体之间制造不和、不信任和怨恨。他们可能会伪造信件或采取类似的措施来构陷活动人士。

[image]

相关内容请查看本站主题页面：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

主流媒体也会参与其中，他们会报道一个团体中有一个告密者（线

人），而事实上这个团体中并没有告密者，或者歪曲个人或团体的政治或历史，以疏远潜在的盟友，或者反复强调一个运动的两个分支之间存在冲突，直到他们真的互相不信任 ...... 如果您像我们一样已经跟随 Wikileaks10几年，您不会对这些做法陌生，在该组织身上发生的一切集中了全世界所有最典型的 “秘密行动” 的操作手段。它应该是个警惕教材。

[image]

返回：

返回：

返回：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

返回：[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

同样，培养适当高度信任和信心的精明安全文化，应该使渗透者的挑衅在个人层面上几乎不可能发生；当涉及到不同策略的支持者和不同条理的组织之间的关系时，请记住团结和策略多样性的重要性，并相信其他人也是这样做的，即使媒体的描述表明不是这样。

不要把传言或新闻报道当作事实来接受：每次都要去找消息来源确认，并且要有外交态度。

18、不要被虚张声势所吓倒。

警察的关注和监视并不一定表明他们知道您的计划或活动的任何具体内容：通常情况下，这表明他们不知道，并试图吓唬你，让你不要继续和其他人合作。

[image]

您应该意识到敌人只是想让您痛苦，让您为他们做事。拒绝他们的阴

谋。

[image]

19、时刻准备着您被监视的可能性，但不要误以为吸引了监视就等于行动有效！

即使您所做的一切都是完全“合法”的，但如果情报组织和警察觉得您给他们的主子带来了不便，您仍然很可能受到他们的关注和骚扰。

从某些方面来说，这可能是好的，这些间谍要监视的人越多，精力就越分散，他们就越难锁定和中和真正的行动者。但是，同时，不要沉浸在被监视的兴奋中，不要以为当局越关注你，你对他们来说就越具威胁性，这是错误的！—— 他们可没那么聪明。

[image]

最好的策略是那些能够接触到人们、提出观点、发挥影响力的策略，同时不会出现在当权者的雷达上，至少在镇压战术为时已晚之前不会出现。

最理想情况下，除了当局之外，您的活动应该被其他所有人熟知。

20、“沉默”不是无声。

安全文化涉及到沉默的准则，但它不是无声的准则。

我们在反抗斗争中大胆探索的故事必须以某种方式讲出来，让每个人都知道抵抗是一种由真人付诸行动的真实可能性；必须公开动员起义，让未来的革命者能够找到彼此，让埋藏在群众心中的革命情绪找到浮出水面的途径。

[image]

一个好的安全文化应该尽可能地保存个人在地下活动中安全所需的所

有秘密，并且同时，又能为激进的观点提供可见性。

今天活动家环境中的大部分安全传统都来自于过去三十多年前的动物权利运动和地球解放活动；因此，它完全适合于进行孤立的行动者小团体的需要，但并不总是适合于更多的旨在鼓励普遍的不服从的公开动员。

在某些情况下，公开动员可能是有意义的，以便激起广大群众的参与，从而提供人数上的安全性。

[image]

返回：[image]社交媒体上的行动主义安全性:框架手册

21、在躲避敌人侦查的需要和潜在朋友接触的需要之间进行平衡。

从长远来看，仅靠保密是无法保护我们的—— 他们迟早会发现我们所有人；同时，如果没有人了解我们在做什么、我们想要什么，当局就能肆无忌惮地清算我们。

届时，必需有一支知情的、同情的（希望也有类似装备的）公众力量，才能帮助我们。

在实行直接行动的社区中，总应该有入口，让越来越多的人可以加入进来。当然，那些做真正严肃的事的人应该把这个入口留给自己，但每个社区也应该有一两个人公开倡导和教育大众关于直接行动，并能谨慎地帮助值得信赖的新同伴与其他开始行动的人联系起来。

22、当您计划一项行动时，首先要确定与之相适应的安全级别，并从那里开始采取相应的行动。

要学会衡量某项活动或情况所带来的风险，以及如何适当地处理这些

风险，不仅可以帮助您远离监狱的关键部分，还有助于知道自己可以不担心什么，这样就不会把精力浪费在不必要的、繁琐的安全措施上。

[image]

返回 - 相关教程：[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局

请记住，一个给定的行动可能有不同的方面，需要不同程度的安全保障；一定要把这些 区别开 ！

下面是一个可能的安全等级评定系统的例子，从窄到宽：

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

根据上述安全级别选择最适合您的一种。

并且，根据您所需的安全级别选择将使用的通信方式同样非常重要。下面是与上面概述的系统相对应的不同级别的通信安全性的示例 —— 要对应着看哦：

1、除了亲自到参与人员的住所而不是通过互联网、在确认无监视的环境中再讨论行动本身，否则不得就行动进行交流；除非绝对必要，否则不得讨论行动本身。

[image]

相关自卫战术页面：[image]户外无设备对话 ；[image]反监视 ；[image]监视器排查 ；[image]藏匿点或安全屋 ；[image]突袭应对措施

2、在小组会议之外，参与人员可以在确认无监视的空间中自由讨论行动。

3、允许在没有被物理监视的住所中讨论行动。

4、通过加密的电子邮件或端对端通信应用进行交流是可以接受的。

[image]

返回-工具：[image]隐私型电邮提供商的列表 ；[image]Tor上的加密邮件服务 ；[image]适合高风险用户的通信平台 ；[image]匿名 SIM/SMS 服务 ；[image]在任何聊天工具中发送算对端加密信息

5、人们可以通过电话、电子邮件等方式谈论行动，但是，要注意不要泄露任何重要细节 —— 比如 谁、什么、什么时候、在哪。

6、电话、电子邮件等都是可以接受的；电子邮件列表、向报纸发布公告等等都可以，要根据具体情况，可以接受，也可以不接受。

7、鼓励通过各种可能的媒介进行沟通和宣布。

[image]

如果您不想让危险信息流传出去，并且您在每个项目中都遵循了适当的安全措施，您就能很好地完成早期工作。

美国活动家 **Abbie Hoffman** 曾经描述的革命者的首要职责就**4**个字：不被抓住。

祝您的行动主义冒险一切顺利，请记得—— 这些建议都是您自己想出来的，不是我们告诉您的。

[image]
[image]

反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

[image] 关键词	交往 人际安全 协作 反渗透 团队 威胁响应
[image] 关联	[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01
[image] 创建时间	2025年1月1日 9:00 (GMT+8)
[image] Description	反渗透和协作

[image]

“威胁知识库”对应“镇压手段”页面：🦁渗透者 ；□告密者（线人）

对应“自卫措施”页面：[image]背景调查 ；分身 ；[image]关系网络图谱

[image]

目标是穿过沼泽地。

而不是对付每一条鳄鱼。

所有内容远非详尽。希望本站各栏目的研究主题能够在社会运动内部引起更广泛的讨论，激励各方有志之士更努力地投入资源以探讨如何保护公民反抗运动的可持续发展。

[image]

首先，可以肯定地说，基本上不存在没有被渗透的反抗和反叛组织，每一种民间组织都有被安插线人，不论您是行动派还是表达派、主张改良还是革命，对维稳部署来说并无本质区别。

人们会担心吗？肯定会，就如您在中国看到的，彼此间的信任程度不断下跌，"抓特务" 搞得乌烟瘴气。这是渗透威胁最容易导致的反应。其中一些反应不仅不明智导致了打草惊蛇，并且还破坏了自身组织的凝聚力和抵御能力。

我们在中国了解到的渗透疑点更像是大撒网，当局似乎旨在不放过任何一个异议社群 —— 请注意，这里所指的 "疑点"，很大程度上还没有确切的证据能表明某人是渗透者，但有明显的迹象值得怀疑。调查和确认渗透从来都不是容易的事，除非有吹哨人，曝光间谍部门的机密文件，或者幸运的遇到了敌方分赃不均的内讧，从而让您得到嫌疑人受雇于镇压机构的证据。否则，足够长时间的观测和取证、甚至试探测试，都是必不可少的。

人们的反应大体上可分为两种，一种是以大方向为目标，选择性忽视疑点；另一种是，由于厌倦和疲于勾心斗角，而退出行动。这是自然的反应，但显而易见的都在不同方面失败。因为，的确可以有更好的办法来抵御渗透和告密的威胁。

这就是本栏目想要与大家探讨的主题。

[image]

以下是几点简述（并非完整策略）

1、渗透者会用你的语言来对付你。

简单说，你支持什么，他们就喊什么，以此在意识形态上与目标受众产生共鸣；但同时，他们的足迹却完全违背他们声称拥护的原则。这种手段就在外观上为支持者制造了混乱，因为外界将您与渗透者看作是 "同一阵营"、属于同一场运动。

对此，您需要做的只是将注意力放在人们的行为上，而不仅仅是他们的言论。您将清楚看到这点。

2、渗透者会在行动策略上强加干预。

是干预，而不仅仅是建议或商讨。他们会将矛盾向组织内部聚焦，比如主张“整肃”，挑起内部纠纷，把注意力从运动本身和组织目标上转移开 —— 对人不对事。

对此，您需要做的是始终将行动的大方向放在心中最重要的位置上，拒绝一切“跑题”的主张，您就可以自然屏蔽渗透的影响。不论您是否识别出了渗透者，或什么时候识别，都不再重要。

假定渗透的必然性是完全明智的。您能做的最有效的策略之一就是让渗透即便存在，也无法搞破坏。

3、躲在别人后面。

渗透者也会参加前沿活动，但他们的目的是产生干扰、或者破坏行动/群体。并且更多的是，他们操纵和挑衅其他人无意义的暴力冲动，同时为他们自己创建一个隔离层。

对此，您需要做的只是观察和识别任何一种建议，如果提建议者自己并不行动，那么您可以谨慎考虑这一建议。

别忘了，行动目标始终是解决问题，而不是制造新的问题！

4、不断煽动琐事。

流言蜚语、背后嚼舌头、人格暗杀 …… 渗透者会以各种形式转移人们的注意力，致力于在大群体中分化出更小的阵营。甚至不断分化，以制造和加深不信任。

对此，您需要做的是强调宗旨 —— 我们是一个团体，是一支队伍，我们不应该让任何一位队友落后和被边缘。唯一能从我们的撕裂和分化中受益的人是我们的对手。

学会协调，通过对话解决矛盾，而不是被分化扩大矛盾。

5、伪装积极。

渗透者会努力成为最靠拢运动中心的 “积极人士”，以便使他们对您的抹黑和栽赃更加 “真实可信”。

如果您是某种程度上的运动中心、是领导者，对此，您需要做的是警惕那些单方面告知您关于其他队友的阴暗面的行为，不要仅仅因为有人打小报告就对涉及其中的队友产生怀疑，您应该亲自去调查、亲自与涉及其中的队友交流。

尤其是，再一次强调，不要仅仅去听人们怎么说，要去看，看人们怎么做；不要追求每一位合作者都是道德完美的，这完全不现实；相反您需要致力于去创造条件以激发人们的积极性，让合作者的自发行为/行动吻合大家共同的战略目标。

如果您是被渗透者抹黑的那个人，请与您的组织领导者交流，依照上述原则判断领导者是否称职。

6、渗透者会扩大攻击面。

任何与您见过面的人、甚至仅仅是搭过讪的人，都会被奇迹般地联系到一起，用来攻击您的私生活，当您的注意力集中在摧毁庞大的、腐败的权力结构并暴露大规模的不公正时，渗透者所采取的琐碎焦点将完全集中在您个人身上。

渗透者的问题之一是他们所做的很多事都是在幕后的。因此您的追查要想将信息连贯起来可能需要花费不小精力。所以当您拥有可靠的信息表明存在恶意者正试图破坏组织或抹黑活动家、公开和泄漏信息以破坏组织的安全基础设施时，一定要提高警惕，并启动必要的防御。

请注意，并不是任何一种矛盾都应该怀疑。您必须将人格冲突、个人私怨、巧合或观点分歧，与有目的的渗透操纵区分开！这只有您能做到，因为您了解与您交互的人的特点 —— 反之，如果完全不了解，那就不应该与其交互。

接下来请进入详解部分。

列表

[image] 安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

[image] 关于渗透 …… 一些基本须知

[image] 什么是“秘密行动”？政府间谍会怎么折腾你…

[image] 针对反抗运动的政治渗透：政府线人如何操作

[image] 秘密与谎言

[image] 了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image] 不放弃，不出卖：关于酷刑和证词

[image] “我的”朋友还是“我们”的朋友？：如何执行担保措施

[image] 别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

[image] 为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力

[image] 卧底警察识别手册2025版

[image] 宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切

[image]
[image]

关于渗透 …… 一些基本须知

[image] 关键词	人际安全 反渗透 反监视 团队 数字安全 防御
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ； 渗透者 ；告密者（线人）
[image] 创建时间	2025年1月2日
[image] **Description**	反渗透和协作

不要认输。不能认输。因为只有认输才是真的输了。此外的一切都不是输。

- Table of Contents

  镇压手段
  监控
  渗透行动
  谣言
  虚假通告
  媒体误导
  骚扰
  破坏活动
  准军事组织
  致命武力
  防范渗透的措施
  1.
  2.
  3.
  4.
  5.
  6.
  7.

8.
9.
保护计算机安全
避免陷入偏执

[image]

为了帮助活动人士提升对此议题的认知，本文将系统梳理国家为瓦解对抗性社会组织结构、将反抗意识形态追随者定性为‘犯罪分子’，所采用的各类镇压战术。

所谓的“反情报计划”（COINTELPRO）专门用于瓦解异议政治团体，通过间谍活动、挑拨离间、及信息操控，以实现目标。全球大多数国家均曾采用这些手段，几乎没有例外。因为这是“国家”的本质。

具体案例如下。

镇压手段

监控

情报与安全机构利用现有技术对活动人士实施全面的监控，首先是为建立司法档案做准备。在中国被称为网格管理、枫桥经验。但不论叫什么，其手段都大同小异。

主要手段包括：拍摄照片、录像、车辆跟踪、拦截/窃取通信电邮及信件、自动记录行踪等等，包括基于大规模监控的信息资源，这些都是针对社会运动积极分子的常用策略。

警方通常会渗透手机通讯、对目标人常去的场所进行固定监视、窃听对话，并通过所谓“信息共享”以整合各类渠道的情报。

电信公司及多数私营通信企业都会配合国家实施此类监控，全世界都如此没有例外。

[image]

返回 - 相关镇压手段详述：👂窃听 ；📍定位追踪 ；📹偷拍 ；[image]隐蔽的监视设备 ；[image]警方档案(网格) ；[image]视频监控 ；□网络映射 [image]物理监控（上岗） ；💂公开监视 ；[image]隐蔽监视 ；🎯有针对性的数字监控 ；[image]服务提供商协助调查

每个条目中都有相应的自卫措施。

渗透行动

国家通常在民众示威活动或集会中安插卧底便衣。有双重意图：其一，记录与会人员及集会讨论的内容，其二，挑拨参与者关系以淡化议题。

其实相比下便衣不难辨认。因为鲜少有人参与了集会却对反抗的主题毫无兴趣或者对相关人员一无所知。由于情报机构通常派遣愚钝的或新晋警察执行此类任务，所以，与他们简单交谈下基本上就能辨别谁是便衣。

同时必须知道，条子的常用伎俩更多是利用□告密者（线人）。

线人本是目标反叛团体的内部人员，却为了金钱、恩惠或解决司法问题（被捏住了小辫子）而向情报机构告密。

[image]

线人是极难识破的。历史上无数无辜的活动人士在愚蠢的抓特务内讧中被诬陷为线人。

内讧的草木皆兵在上个世纪曾经成功摧毁了武装反叛组织。只有镇压

者在坐收渔利。

鉴于历史教训，当今激进派行动团体往往规模更小，更多建立在高度亲密关系的亲密团队模式基础之上，甚至以家族/家庭为纽带。“亲密团队”关系结构也是无政府主义革命理念中的重要部分。

还有一种渗透形式相比下容易辨别，即：首次参加集会的“新人”，却不顾行动战略和谈论议题而一味地强推无意义的极端或暴力行动。这些人因颠覆性言论和脱离现实的疯狂提案而格外显眼。

对此做出准确判断的前提是，您和队友具有强化的战略共识，并对战术有效性判断有着一致的标准。

建议将此价值观纳入安全文化中战略共识部分：https://iyouport.substack.com/p/ad0?utm_source=publication-search

谣言

线人和渗透者的存在助长谣言的传播。

传播虚假消息意在渲染疑云，制造人际疏离，从而瓦解社会阵线或集体组织。

这些无端谣言专门用来诋毁组织中的领导者及其中的积极人士。

[image]

人际是主要的安全问题。相关探讨详见本站 🎀人际安全&关系结构革命-RelationshipsRevolution

虚假通告

情报机构还经常编造误导性的文件，在活动家及其关联组织间制造混乱。

其核心战术是制造内部矛盾，以引发组织自行毁灭。

例如，智利检察官曾虚构出一个被称为“革命无政府主义阵线”(FAR)的组织，该组织通过挑衅性认领虚假的行动并煽动与智利非正式团体的争论，最终导致真正的反叛团体被瓦解。

想象一下，如果有人打着“无政府主义者”的旗号滥杀无辜、或者打着“女权主义者”的旗号捍卫统治压迫的秩序，再或者以“激进派”的名义对不同战略的其他反抗运动发起暴虐冲击 …… 等类似状况，会令您对曾经信仰的理论意识形态产生怀疑吗？

希望不会。希望您不至于如此容易被操纵。

因为这些手段都是统治者常用的镇压战术。

[image]

还是那句话：不要看一个人自称什么，不要听TA高喊哪些口号或者对哪些理论大书特书，而是要看TA具体做了什么 —— 尤其是在与其自身利益密切相关的人生决策上此人做出的选择，才是其本质的体现。

媒体误导

部分职业媒体与情报机构紧密合作，通过预设示威者和活动家的负面形象 —— 指控反抗者从事“破坏活动”、或者诬陷反抗者充当“敌方特工”、称其为“失控分子”或“反社会分子”—— 抹黑以塑造舆论。委内瑞拉电视节目《La Hojilla》就是典型案例 ——其主持人（一位知名且屡获嘉奖的警方线人）自诩为检察官、法官，对反对现政府的异见者大肆批判甚至审判。

中国用户熟悉的“上央视”也是同样的手段。

无政府主义者厌恶职业媒体的原因还包括 —— 职业媒体经常传播关于抵抗团体和倡议的错误信息，或发布关于活动家的不真实信息，企图抹黑反抗者对所坚持事业的承诺。

正因如此，反制信息成为关键武器。反抗组织应该有自己的官方声音，而不是一味依靠职业媒体传达话语。

战术推荐：https://iyouport.substack.com/p/b89?utm_source=publication-search

[image]

返回：[image]和媒体说话时如何避免陷阱：街头实战指南 S05E13

返回：

[image]

返回 - 书：

返回 - 书：

骚扰

情报机构更常用的手段还包括接连不断的骚扰，以此来对目标人施加压力。

例如向其雇主举报目标人是“反社会激进分子”，或者在目标人的熟人圈子中散布谣言，使目标人被信任的社交孤立、甚至受迫害。诸如“性变态者”、‘强奸犯’、“吸毒者”等等指控屡见不鲜。

另一种骚扰形式是国家机构锁定活动人士身份后，以任何借口实施逮捕或审讯。许多情况下，逮捕行动会伴随“👎栽赃 ”毒品或其他违禁物品（燃烧瓶、爆炸物等等），旨在迫使当事人放弃抗争。

破坏活动

警方组织（或其关联人员）对活动家的集会场所实施破坏，并盗取物资。

此举旨在向支持者散播恐惧与挫败感。

准军事组织

情报机构组建准军事团体，为其配备武器并进行训练， 以执行那些穿制服的镇压机器不便在“宪法合法性”框架下实施的“脏活儿”。

在委内瑞拉，此类组织表现为邪恶的“战斗军团”或巡逻贫民区的各类“热门团体”。

致命武力

当社会运动中的某人声名鹊起，且体制权力无法通过其他手段将其控制住或收编时，当局便诉诸暗杀异见者——或雇佣暴徒（伪装成普通罪犯），或制造所谓冲突事件（此类事件经客观调查不难揭露）。

□

延伸：https://iyouport.substack.com/p/091?utm_source=publication-search

[image]

防范渗透有两个关键：

1. 及时识别“外人”；

1. 尽可能不要过早的让对手识别到您的亲密团队组合。至少要保留足够的幕后接应。

防范渗透的措施

1.

集会或亲密团队的聚会期间，最好不要携带自己的手机。

请将手机置于远离敏感聚会/集会区域。

手机不仅被用于扣押取证和追踪定位，尤其会用于构建异见者的社交关系网络，以便在需要的时候连锅端。

2.

进入集会地点之前，先绕行侦察外围区域，留意可疑活动迹象。

便衣警察通常可通过体格特征、谈吐方式或格格不入的气场识别到。他们极少直视对方眼睛，且解释时常语无伦次。

3.

群发邮件时务必使用密送（BCC）功能，即便邮件遭截获也不致暴露

其他收件人。

4.

可通过网吧等公共服务发送通讯，防止情报机构获取您的IP地址。

[image]

返回：[image]与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧

返回 - 自卫措施：[image]数字技术限制和最佳实践

5.

行动者间的 亲密无间与互信互助 是抵御渗透与镇压的最佳良方。

宁可人数精简而安全可靠，不可追求人多而松散无序。

永远记得，我们只有彼此。

6.

切勿助长虚假信息的传播，禁止流言蜚语或恶意嚼舌。

不要说无凭据的话。如果您有疑心，那就让自己隔离危险源，同时仔细观察以寻找详细证据。不要在无凭无据的情况下传播猜想。

7.

保持警惕 —— 但避免陷入偏执 —— 及时察觉和防范渗透与挑拨。

8.

若察觉遭到监视，务必告知其他战友。

9.

切勿与警方交谈。

请谨记您始终有保持沉默的权利。

切勿与镇压系统合作。

出卖朋友换取减刑等承诺都是巨大的谎言。一次妥协就将终身无法摆脱魔鬼的利用。

保护计算机安全

不要被数字产品出卖。所有数字产品都是埋伏在您身边的间谍 —— 高科技渗透者。

[image]

有些情况下我们不得不使用数字产品，所以保持一个原则很重要：即 **[image]** 数字技术限制和最佳实践 。

本站“操作安全性”主题是关于数字安全自卫措施的建议；如果您希望进行系统性数字安全培训，请使用本站S01、S02、S03系列教材。

对任何觉得麻烦的人说：一些简单的卫生习惯就能带来安全程度的明显提升 —— 比如，把您的谷歌邮箱换成Riseup（www.riseup.net）；对您在意的任何文件使用PGP（www.pgp.com）加密；习惯于在Matrix中而不是微信中形成并抚育您的亲密团队关系网；从Tails启动以进行您的敏感工作，而不是Wins或macOS ……

再次强调，如果您正在团队/社区中组织培训工作，非常建议按照本站的教程序号顺序进行。

避免陷入偏执

部分活动人士因过度偏执而完全丧失行动力，最终放弃抗争沦为社会旁观者。

这是一种悲惨的自我销毁！

我们必须深刻理解上述原则，在充分认知风险的前提下做好准备，并采取周密的行动计划，从而降低脆弱性。必须清醒地认识到：任何集体抗争都可能成为警方监控的目标，这是社交动态的必然组成部分。武装控制与镇压机构正是为压制各类异议而存在的，因此抗争者必然成为其目标；但我们拥有更崇高的价值——为积极社会变革坚守的信念。切勿让疲惫与恐惧阻碍前行！

[image]
[image]

什么是“秘密行动”？政府间谍会怎么折腾你...

[image] 关键词	反渗透 反间谍
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；🦁渗透者 ；□告密者（线人）
[image] 创建时间	2025年1月4日
[image] **Description**	反渗透和协作

不仅军方会进行秘密行动，警察和间谍也是如此。众所周知的就是这些镇压机器对抗议者和政治运动的渗透。这些秘密行动是如何运作的？

- Table of Contents

  希姆莱行动
  曼尼拉的轰击
  格拉迪奥行动
  拉冯事件
  中情局在伊朗
  北木行动
  麦克米伦支持叙利亚暗杀阴谋
  警察渗透持不同政见组织的秘密行动
  在英国，付费的线人
  煽动
  卧底监视
  CIA 的间谍工具包是数字化的

[image]

历史并非如此。历史就像一件旧毛衣，慢慢地被拆开。它被缝补过无数次，为了适应不同的人而重新编织，被塞进审查制度水槽下的箱子里任人裁剪成宣传抹布，却总能——终究总能——弹回到熟悉的旧模样。历史总爱改变那些自以为在“改变历史”的人。它那破旧的袖口里永远藏着几招绝活。毕竟，它可是存在了很久很久的。” ~ 特里·普拉切特，《死亡》

秘密行动是如何运作的？事实上80%的操作是拿破仑曾经使用过的策略的复制。场景规划、系统理论的支持应用、博弈论、战争游戏理论、以及许多其他实践性战略思想和战略执行的模式也被使用。

以下这些古老的已知行动是很好的案例研究，80%可在当今的秘密行动、心理战和宣传战中复制。

希姆莱行动

希姆莱行动是党卫队为了在战争爆发时为纳粹德国的具体宣传目标服务而进行的一系列非常规秘密行动。其目的是为了证明波兰对德国的入侵是对德国的侵略。该行动中最知名的是 Gleiwitz 事件。

而且有说服力的说法是，纳粹焚烧了他们自己的议会，即国会大厦，并把责任推在别人身上。德国国会大厦的火灾是分水岭事件，证明了希特勒夺取权力和终结自由的开端。

曼尼拉的轰击

1939年11月26日，曼尼拉的炮击事件是一起军事事件，苏联红军炮击了俄罗斯的曼尼拉村，然后宣布袭击来自芬兰，并声称人员死亡。苏联领导人尼基塔·赫鲁晓夫以书面形式承认，1939年是苏联红军炮击了俄罗斯的曼尼拉村，作为四天后发动冬季战争的基础。

格拉迪奥行动

格拉迪奥是冷战期间欧洲臭名昭著的秘密行动，在九十年代，一个秘密武器藏匿、军事战略和政治阴谋的故事。秘密战争中描述了一系列事件：格拉迪奥行动和北约的驻军后卫。

总理安德烈奥蒂承认，格拉迪奥已发展成为一个广泛的网络分支，在北约内部运作，并在1956年美国与意大利秘密机构之间的协议中受到怂恿。

德国、法国、比利时、荷兰、希腊和卢森堡都承认他们维持了格拉迪奥式的网络，以准备游击队员在华沙条约入侵的条件下突击行动。许多人的代号为 Stay Behind。在希腊，它被命名为 Red Sheepskin。

根据当时的新闻报道，此类行动也存在于英国，挪威，葡萄牙，西班牙，奥地利，土耳其和丹麦，甚至还存在于瑞士和瑞典等中立国家。

1956年与美国机构达成协议的目的是确保西方最大的意大利共产党不能在政府中站稳脚跟。在意大利秘密机构和新法西斯主义者之间存在长期的联系，并且在70年代震撼意大利的主要未解决的恐怖主义行为都被认为是极右翼主导的，而肇事者从未被抓到过。

在一些国家，Stay Behind 网络已经被关闭。希腊的社会主义者说，他们在1981年发现了该网络后来废除了它，并在1985年抄查了武器。在法国，密特朗说他取消了法国分部，但他没有说什么时候取消的。显然，大多数其他欧洲国家的秘密行动网络仍在继续。

拉冯事件

在埃及活动的一个以色列恐怖主义小组在包括美国外交设施在内的多座建筑物中埋下了炸弹，然后留下了“证据”，暗示阿拉伯人是罪魁祸首。其中一枚炸弹过早引爆，以便“判定”肇事者。

几名以色列人后来供认，其中三人后来被以色列人尊敬。

中情局在伊朗

由纽约时报记录，为C.I.A.工作的伊朗人在1950年代制造爆炸事件，冒充共产党人所为，以使该国反对民主选举产生的总统。

北木行动

解密文件显示，在20世纪60年代，美国参谋长联席会议签署了代号为“北木行动”的计划，以炸毁美国飞机，并以“在美国土地上实施恐怖主义行为”的名义归咎于古巴人，以证明入侵古巴是正当的。

由于肯尼迪政府拒绝执行五角大楼的这些计划，因此没有进行这项行动。

麦克米伦支持叙利亚暗杀阴谋

在伊拉克战争将近50年之前，英国和美国又在另一个阿拉伯国家寻求秘密的“政权更迭”，他们被指控通过策划入侵叙利亚和暗杀领导人来传播恐怖主义并威胁西方的石油供应。

文件显示，1957年哈罗德麦克米伦和总统德怀特艾森豪威尔批准了一项中央情报局—军情六处的计划，将假边境事件作为叙利亚入侵亲西方邻国的借口，然后“消灭”大马士革最有影响力的三巨头。

部分“首选计划”内容如下：

> “为了促进解放力量的行动，降低叙利亚政权组织和指挥其军事行动的能力，将损失和破坏降至最低，并在尽可能短的时间内取得预期成果，应作出特别努力

以消除某些关键人物。他们的撤职应该在起义和干预的早期完成。“

警察渗透持不同政见组织的秘密行动

不仅军方会进行秘密行动，警察也是如此。众所周知的就是他们对抗议者和政治运动的渗透。

在英国，付费的线人

由于70年代和80年代的糟糕时期，当系统失去信誉并且皇家检察院拒绝接触任何向警方告密的案件时，规则已经收紧。 [...] “2000年调查权力法”对“线人”的使用进行了监督。在公共当局授权使用隐蔽来源的情况下，该法案的规定适用于苏格兰。

2009年，在英格兰，一位气候变化活动家录制了证据，揭露了一些当局的线人被提供现金以获取有关团体成员和活动的私密信息。

在录音带中，警察声称已经渗透到一些环保组织内部，并表示他们正在接收有关未来示威的领导者身份、战术和计划的信息。活动人员也受到广泛的监视。

在苏格兰信息专员作出裁决后，斯特拉斯克莱德警方被迫公布了向“隐蔽的线人”支付款项的细节，详细情况显示该部队自2004年以来每年支付给线人的金额几乎翻了一倍，当时是145,198英镑，2004年至2008年共支付了762,459英镑。

煽动

在抗议期间，G20警察“使用卧底线人煽动人群”，这类现象并不意外。

煽动就是为了 👎栽赃 ，以证明镇压的合理性。

卧底监视

> 苏格兰场已经部署了秘密警察来监视一个民间活跃人士的关系网络，这些活动家反逃税的热门宣传活动有可能在圣诞节期间关闭数百家商店。
>
> 尽管去年向议会保证只有穿着制服的军官在抗议活动中收集情报，但是，负责监视的便衣最初还是在10月的抗议活动中被使用了。
>
> 没人知道的是，尽管这位33岁的“自由登山者” Kennedy 非常著名，但他还是一名卧底警察，一直在大胆的行动，深度渗透环保活动家群体。“战术”甚至包括滥交行为。
>
> 2011年，第三名卧底警察间谍被揭露，更多关于 Kennedy 在欧洲抗议运动中的关键作用的细节也出现了。显然，他还在爱尔兰、德国和冰岛担任卧底线人。他可能已经要求公关公司 Max Clifford 出售他的故事。
>
> 2015年3月，建筑工会 UCATT 暴露了警察的渗透，并于2014年12月2日提出了 FOI 请求。但是响应被不断推迟...... 2月20日，警方表示他们“无需确认或否认是否提供被要求的信息“，并列举了为什么他们无法透露包括所谓的“国家安全”在内的六方面信息。简称：滥用法律的狡辩。

CIA 的间谍工具包是数字化的

在过去十年中，受过专门训练的 CIA 秘密运营商已经安装了一百多个非常敏感的black bag，旨在渗透外国政府和军事通信和计算机系统，以及一些世界上最大的外国跨国公司的计算机系统。

间谍软件已秘密植入计算机服务器; 安全电话线已被窃听; 光纤电缆、数据交换中心和电话交换机已被挖掘; 在这些操作中，计算机备份磁带和磁盘被盗或被秘密复制。

换句话说，中央情报局建立秘密监视巨型网络的工具现在已被投入公众视野。美国情报界的消息来源证实，自9/11以来，中央情报局的秘密行动使国家安全局能够进入世界各地的极其重要的目标（不知道在美国的土地上是否也有这样的行动）

以上文字的链接部分显示相关故事的更详细报道。

关于卧底监视，推荐以下资料：

- Resisting Surveillance: it's not just about the metadata

https://youtu.be/H8yfDX0Myvw

- The Undercover Research Project aims to create an one-stop resource on political policing and undercover surveillance http://undercoverresearch.net/

- The Campaign Opposing Police Surveillance exists to help co-ordinate,
publicise and support the quest for justice for people affected by
political undercover police spying and to ensure such abuses do not
continue http://campaignopposingpolicesurveillance.com/

- Spied Upon is an upcoming documentary film showing the side of the story of
  those targeted by secret police, while revealing at a human scale
  today’s complex international spying apparatus, a system that has spun
  out of control. We are currently fundraising for final shooting and
  completion of a rough cut in late 2015 http://spiedupon.com/

- Verfassungsschutz abschaffen! http://www.verfassung-schuetzen.de/wissen/verfassungsschutz-abschaffen/

还有一本书：@War: The rise of the military-internet-complex http://cryptome.org/2014/11/at-war-mil-net-complex.pdf

- The War You Don’t See

https://youtu.be/5mDuxFnn2RY?si=mGKaddiWoqpeClNM

- Undercover police officer: ‘How I spied on the Stephen Lawrence campaign’ http://www.theguardian.com/uk/video/2013/jun/24/undercover-police-stephen-lawrence-video

- ‘Why police recruited me to infiltrate the British National party’ http://www.theguardian.com/uk-news/video/2014/jun/23/police-recruit-infiltrated-undercover-british-national-party-bnp-video

- Counter-Intelligence: I—The Company

https://vimeo.com/65148608?fl=pl&fe=sh

- Counter-Intelligence: II—The Deep State

https://vimeo.com/65942057?fl=pl&fe=sh

- Counter-Intelligence: III—The Strategy of Tension

- Counter-Intelligence: IV—Necrophilous

https://vimeo.com/66019647?fl=pl&fe=sh

- Counter-Intelligence: V—Drone Nation

https://vimeo.com/66183267?fl=pl&fe=sh

在中国从来没有看到过对卧底监视如此详尽的揭露证据。 希望以上内容能帮助中国的积极人士参考，关于：什么是证据、和如何拿到证据。

[image]
[image]

针对反抗运动的政治渗透：政府线人如何操作

[image] 关键词	个人 人际安全 关系 反渗透 团队 威胁响应 防御
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；渗透者
[image] 创建时间	2025年1月5日
[image] Description	反渗透和协作

有至少30万名警察参与渗透监视民间政治活动。这些间谍的部分工作包括暗杀政治活动家……平均每6个人中就有一个是政府间谍。

记者实际上是间谍，最活跃的活动家实际上是间谍，就连竞选主席也实际上是间谍 ……

- Table of Contents
渗透是针对政治运动的常态而不是特例
渗透是常态，没有渗透才是例外
过去渗透的目标、战略和战术都有哪些

[image]

2012年3月6日，一名匿名者组织分支机构 Lulzsec 的成员因被联邦调

查局的线人Sabu出卖而被捕，他被媒体描述为Lulzsec“领导人”。

这六名被捕者据称都与 Lulzsec 组织有关，后者因针对索尼、中情局、美国参议院和FBI，以及Visa、万事达卡和PayPal等公司而闻名。

整整一年前，《卫报》发表了一篇文章，标题是 “每四个美国黑客中就有一个是**FBI**的线人”。

文章描述了联邦调查局如何 利用长期服刑作为威胁，将一些匿名者组织和类似组织的成员策反为线人 。文章还描述了该组织是如何被渗透的。

麦吉尔大学教授、数字媒体、黑客和法律专家加布里埃拉·科尔曼在独立媒体组织“现在民主”的节目上说：”曾经有不少关于渗透或线人的传闻。在某种程度上，匿名者组织很容易被渗透，因为任何人都可以加入和参与。因此，这种渗透的传闻已经有相当长的时间了。”

本系列的上一部分内容介绍了渗透者的行为，其他反抗运动如何反击渗透者，以及可以做些什么来减少渗透者所造成的伤害。

本文将介绍政府间谍对政治运动渗透的历史，以及渗透者的目标。

渗透是针对政治运动的常态而不是特例

当回顾政治渗透的漫长历史时，”占领运动” 如果没有被渗透肯定会令人感到惊讶的。现代历史上几乎所有的反抗运动都曾被警察和其他人渗透过，使用了许多我们现在在 “占领 “运动中所看到的同样的策略。

几乎所有运动都是警方监视和破坏的重点目标。

最著名的监视方案是联邦调查局的 COINTELPRO 计划，根据 COINTELPRO 文件，该计划以女权组织、民权组织、反战组织与和平运动、新左派运动、社会主义者、共产党人和波多黎各独立运动等民间组织为目标。

被渗透的团体包括南方基督教领袖会议、有色人种协进会、种族平等大会、美国印第安人运动、学生争取民主社会、全国律师协会、黑豹组织、和地下气象组织。从阿尔伯特–爱因斯坦到小马丁路德金博士等重要领导人，都受到了监视。

渗透是常态，没有渗透才是例外

丘奇委员会记录了联邦调查局进行政治镇压的历史。他们描述了第一次世界大战前的渗透工作，包括1920年代，当时特工们被指控围捕 “无政府主义者和革命者“，以便将他们驱逐出境。

丘奇委员会发现，从1936年到1976年，渗透活动不断增加，主要的方案就是 COINTELPRO。虽然这些国内政治间谍活动和破坏计划本应在1976年停止，但是，事实上，这些计划一直在继续。直到今天。

正如 “异议的代价 “中所报道的，联邦法官 Joan Lefkow 在1991年发现，记录表明，“尽管有条例、命令和同意令禁止这类活动，但联邦调查局仍继续收集那些仅仅涉及行使言论自由公民权的反抗者的私密信息。

一个运动的内部究竟能有多少特务或潜入者？最臭名昭著的案例之一就是1968年的民主党党代会。独立记者 Yasha Levine 写道：”在1968年芝加哥民主党全国代表大会的抗议活动中，吸引了约1万名抗议者，他们被警察残酷地镇压 —— 每**6**名抗议者中就有**1**名是联邦调查局的卧底。

没错，全部抗议者中的**1/6**都是由各种政府间谍组成的 —— 也就是说，大概有**1600**个间谍！

这个统计数字来自于CBS新闻社在1978年获得的一份军队文件，那是在抗议活动发生整整十年后的1978年。据报道，这些渗透者不是被动的观察者 —— 不是仅仅监视和向中央指挥部传递信息，而是参与了与警察的暴力对抗。” [原文强调] 简单说就是制造暴力以污蔑非暴力反抗行动，以令警方的暴力镇压 “有理有据”。

[image]

彼得·卡梅约2003年以绿党身份竞选加州州长，2004年以拉尔夫·纳德的副总统身份竞选，他经常讲述自己1976年竞选总统的故事。

卡梅约在发现自己的办公室被破门而入、他遭受了COINTELPRO的间谍活动后，将FBI告上了法庭。

法官问负责的特别探员，有多少FBI探员在卡梅约的总统竞选活动中工作；答案是：66名探员。 卡梅约估计，他在全国各地只有大约400名竞选人员。

再一次，这依旧是平均每**6**个人中就有**1**个间谍的渗透率。

卡梅约发现，这些特工中甚至就包括他的一名竞选联合主席。他还在竞选办公室里发现了窃听设备，还有文件显示，**FBI**从他**18**岁还是学生活动家的时候就开始跟踪他了。

FBI 的渗透活动得到了地方和州警察的支持。

地方警察操作的渗透有着悠久的历史，可以追溯到1886年的干草市场暴动。

除政治活动外，他们还参与了 对工会的渗透活动，尤其是在罢工运动期间 。

在全国各地最常见的是所谓的 “红色小队”，据1963年的报告估计，有至少**30**万名警察参与渗透监视民间政治活动。这些地方警察与**FBI**一样，都是专注于监视同类型的人。

占领运动的另一个前身是1968年 “复活城“（Resurrection City of the Occupy），是由“穷人运动”组织的 “爱与兄弟情谊社区“，占领了华盛顿特区商场四个月，是在小马丁路德金博士逝世前制定的计划。复活城抗议行动被FBI、军方、公园警察、特勤局和华盛顿特区警察局等层层渗透。

当时的联邦调查局局长（历史上最臭名昭著的）胡佛让特工们带着假的媒体身份去参加记者会，在营地周边派驻**FBI**特工，并授权进行昂贵的线人计划。

在FBI之后，对复活城最昂贵的渗透是军方的情报人员进行的非法监视计划 —— 拦截无线电信号，监视无线电通讯，并截获了所有的通讯，然后将这些通讯传给了**FBI**、特勤局、特区警察和公园警察。

渗透战术还在继续，甚至今天已经升级了。

[image]

美国公民自由联盟在的一份报告中写道：“今天，政府仍然继续以我们国家的缔造者们无法想象的方式对公民进行间谍活动。联邦调查局、联邦情报机构、军队、州和地方警察、私营公司，甚至是消防员和紧急医疗技术人员，都在收集大量关于普通公民的个人信息，这些信息可以用来构建庞大的档案，通过所谓的反恐联合工作组、融合中心和公私(监控)合作等新机构，只需点击下鼠标，就可以广泛共享……像过去一样，警方的情报活动过度热衷于针对政治活动家、种族和宗教少数群体以及移民”。

也有多份报告称，中央情报局多年来一直与纽约市警方合作，这种活动几乎可以肯定是非法的。

在911后的世界里，不仅维稳预算大幅增加，而且对间谍活动的限制也被削弱了，法院的审查也变得越来越少。

政府往往与企业利益相关，他们正在收集所有公民的海量数据，并针对各种团体和个人进行情报收集和渗透。

间谍活动的范围之广，超出了这篇简短的文章所能研究的范围，但美国公民自由联盟（ACLU）提供了一个逐州的审查。

我们将在相当长的时间内无法知道目前渗透的程度和政府特工的活动，但在911后的世界里，随着创纪录的情报预算和庞大的新的国安官僚机构涌现，间谍活动很可能比以往任何时候都更加广泛。

再加上与两个政党捆绑在一起的寡头公司和政治组织的私人维稳，渗透的范围很可能超乎每个人的想象。

[image]

返回 - 镇压手段：[image]服务提供商协助调查 ；[image]移动网络运营商 ；[image]其他可能出卖您的服务商和机构 ；🎯有针对性的数字监控

过去渗透的目标、战略和战术都有哪些

渗透活动最常见的目的是收集内幕信息的情报功能，但是其目标通常更具有攻击性。

根据 COINTELPRO 文件，胡佛命令FBI特工们要 “揭露、破坏、误导、诋毁或以各种其他方式瓦解这些运动及其领导人的活动”。

COINTELPRO 的目标也是为了 “揭露、破坏、干扰、误导或以其他方式使民间组织失效”。联邦调查局的外勤人员被指示：

1、通过对活动家中的积极分子进行调查，然后向公众发布其负面的个人信息，为目标群体创建负面的公众形象 —— 也就是《人格暗杀》。

2、通过让特工人员激化种族矛盾，或发送匿名信制造民间组织的内部矛盾，从而瓦解反抗组织的内部 —— 也就是挑拨离间、制造混乱和不信任。

3、通过散布其他团体偷钱的谣言，在团体之间制造分歧 —— 这是为了拆散联盟的可能性。当民间组织之间能够联合起来的时候，才是当权者最恐惧的时候。

4、通过向非营利组织施压，限制其获得公共资源的机会，切断对非营利组织的资金或物质支持 —— 简称，饿死异议。

5、渗透进入的特工在策划抗议和抗议活动期间宣传针对警察的暴力，以此来限制组织抗议的能力。

6、通过人格暗杀、伪造的逮捕（也就是没有法律依据的的逮捕监禁，以恐吓为目的）、渗透监视等方式，限制个人参加集体活动的能力。

COINTELPRO 的文件中披露了许多FBI意图阻止反越战的群众抗议的案例。

为了完成“任务”，使用了许多肮脏的手段。

这些文件指出：“这些手段包括促进反战势力之间的分裂让他们无法联合，鼓励对活动家进行迫害，并由此来推动暴力对抗，以取代大规模的和平示威。”

渗透收集情报、故意破坏和瓦解社会运动的行为，一直都是很常见的。

在历史上，当贫富不均的程度已经达到如此惊人时、最富有的400人所拥有的财富和最底层的15.4万人的财富相同时、当失业率和法拍屋率居高不下时，当几千万人买不起医保、学生上不起大学时，当权势担心人民会起义时 …… 这一切间谍行动就会发生。

近年来发生的所有事件，特别是 “占领“事件，显示出这场起义已经开始了。当权者会利用现有的一切工具来阻止 “占领“，包括渗透破坏、分裂和误导。

本系列下一部分的内容将描述渗透者的常见行为，以及其他社会运动如何试图将渗透的影响降到最低。然后将研究 “占领 “的基本结构，并分析其在渗透的背景下的优缺点。

[image]
[image]

秘密与谎言

[image] 关键词	个人 亲密团队 人际安全 保密分级 反渗透 团队 心理安全 权力关系
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病；[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌；[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09；🙆渗透者；□告密者（线人）
[image] 创建时间	2025年1月6日
[image] **Description**	反渗透和协作

如果您也曾亲历过拉帮结派勾心斗角，尤其是，如果您不幸正是那个被排挤的人、甚至因此被迫放弃了自己呕心沥血的革命事业，就如本文的作者一样，这一集内容值得我们深思。

- Table of Contents

紧密相依
附言（实用建议）
1.
2.
3.
4.
5.
6.
7.
8.

[image]

你有没想过，当心理安全和人际安全发生冲突时，你会选择顾哪一边？……

这可能是一个残酷的问题。

紧密相依

安全文化最美好的状态是能够共同创造保护我们彼此的实践，通过建立信任让关系开放，从而促进协同行动的可能性。这让人感觉像是在滋养一种共谋和团结的精神，不仅限于我们身边的同志，更是延伸到世界各地与无数无政府主义者和反叛者相连。每一位散播反抗火种的人，都与他们信任的同志一起守护着宝贵的秘密，正是这些秘密让我们的斗争永续。

然而，在实践中，这不可避免地会充满混乱和艰辛。

要发展出共享互助的、无等级无支配性的理想相处方式，其过程可能会显得笨拙甚至令人沮丧。我们的沟通技巧和自我反思能力不可避免地在考验中磨砺。秘密压在我们心头，使我们孤立。它是一个负担，尽管是我们尽力共同承担的、必要的负担。

[image]

但当安全文化停止动态流动，不再植根于我们彼此的承诺与斗争的共同实践，而演变成一种模棱两可的、甚至主要是美学上的亚文化仪式时，它就变成了一种腐蚀性的液体，浸入并加深了渗透这个世界的威权主义、等级制度和自我中心的裂痕。

这可能会危及经过多年培养的共同行动潜力，也会危及我们每个人的安全 —— 安全文化本该守护的核心。

当这些裂缝崩裂扩大时，它们就很容易被用作渗透的切入点。当我们

的共同立足点在我们脚下崩塌时，我们就有跌落的风险，彼此间的关系被撕裂的风险，被统治系统等级制度秩序重新吞没的风险。

《秘密与谎言》的作者就是一位跌入裂缝的人。在暂时远离这种保密文化之后，作者反思了这种文化可能存在的问题，尤其是，它本可以或应该可以呈现的另一种面貌。

作者为我们提供了一个宝贵的机会，去重新审视我们自己的行为准则和规范 —— 它们是保护我们彼此和共同潜能所必需的吗，还是仅仅为了表明我们属于某个排他性的小圈子？两者往往同时存在，但（通常是真实的）镇压威胁在我们脑海中制造的刺耳喧嚣可能过于响亮了，以至于淹没了所有的个人和集体的反思。于是我们回避对这个痛苦问题的追问 —— 我们对同志的信任、我们的自我认同，抑或二者兼具，是否如此脆弱，以至于我们需要这些持续的信号才能感受自身的价值？

[image]

我想在作者的反思的基础之上，再补充一个我观察到的会助长这些动态的规范。激进派反叛者常以（必要的）秘密为借口，来为自己情感上的斯多葛式封闭做辩护。他们是如此坚定的革命者，以至于他们的整个生活都被秘密所笼罩了。

[image]

这种方法并非来自无政府主义革命图景，相反，是承袭自我们都成长于其中的父权文化，这种文化教导我们压抑情绪的能力是衡量力量的标准。

恰恰相反，这种文化规范已被证明是我们运动中的一个巨大的脆弱点，并且是完全不可持续的。那些精于掩埋情感的同志逐渐变得病态、孤立、偏执甚至具有虐待性，而那些不能或不愿将内部挣扎隐藏起来的人则被推向边缘。

这并非否定根据心理/情感状态重新评估和调整安全协议的正当性或必要性。诚然，有时我们确实无法承受行动压力，那就不应该参与其

中。相反，我们对激进派圈子中精神和情感健康的理解不应塑造军队式的那种理想士兵形象，而是应该反映我们反威权和反父权的价值观，以及我们对自由互信的亲密关系的渴望。我们每个人都有情感，我们都被这个世界折磨得支离破碎，都需要面对这些困境——不仅是那些明显精神失常者。而且我们的愿景必须着眼于长远—— 如何让正在构建的关系及其催生的美丽反抗持久延续，而非仅限于短暂爆发？

正如我们在街头需要战略智慧一样，我们也需要情绪智慧来避免传播这个社会灌输给我们的毒液，并以富有创造力的方式应对不可避免的冲突。这种智慧必须通过实验、分享和关怀来积极培养，而所有这些都取决于我们学习和成长的意愿。

我们许多同志对心理健康专业人士和机构持怀疑态度，这是情有可原的 —— 因为他们厌恶精神病机构的暴力，或者曾经直接或间接被这些机构伤害过，或两者兼有。不是每个人都需要看治疗师，对于需要的人来说，机构心理咨询也并不是万灵药。重要的是达成共识：我们都有责任去寻求某种形式的支持。

[image]

有很多事情我们不能谈论，但这正是我们更需要处理可以谈论的事情的原因。

世间有太多禁忌话题，但正因如此，我们更应直面可谈之事。

童年创伤、人际冲突、被遗弃的恐惧、成瘾行为、及其他有害应对机制、被囚禁的创伤 —— 这些未解决的问题会悄然侵蚀心灵，尤其在反抗者时常必需经历的高压时期。

我最近偶然听到一段对话，A说每个人都需要去做心理治疗，而B回答说：“反抗项目就是我们的治疗”。另一些朋友研究了躯体疗法和如何调节神经系统。纽约的同志们开始了共同咨询小组，训练自己在一个彼此信任的环境中互相提供支持。有针对酷儿群体、成瘾者家属、性暴力幸存者的支持小组。寻求支持的方式有很多种，谈话疗法只是其中之一。所以当一位同志拒绝尝试或找借口时，我将其视为一个危险

信号，也是潜在共识的一个重大障碍。即便当下无法为自己做到，我们也应当为同志们努力尝试。

—— Ungrateful Hyenas Editions

我们都带着恐惧降世

至今仍在寻觅言语

来描述那份痛楚

我们紧紧依偎

像雨中的鸽子

（紧紧相依）

互相用羽翼温暖胸膛

（紧紧相依）

用磨损、开裂、沾污的喙

（紧紧相依）

所以这首歌献给那些迷失的人

（紧紧相依）

和那些逝去的、那些离去的人

（紧紧相依）

我们所有破碎的兄弟

（紧紧相依）

和跌倒的爱人

（紧紧相依）

向雨水吐着口水

（紧紧相依）

—— *“紧密相依” (Hang On to Each Other),* 加拿大摇滚乐队银山锡安

接下来的这篇文字来自一位参与直接行动和非正式组织的无政府主义同志。在起义亲和（insurgent affinity）的关系中，当欲望与爱意交融于共同进击这个专制社会的真诚冲动时，我们必须关注我们行动的后果，以及我们所牵涉的人。要理解统治秩序的即定逻辑。当万物终将崩解之时，我们必须找到维系彼此的方式，避免被瓦解抗争意志。

[image]

[image]

> "冲突的心理维度与物理维度同等重要。冲突是意志的较量，既发生于战场亦存在于人心。冲突是权力的角逐。权力可表现为政治（意识形态）、军事或经济（物质）形态。基于意识形态的冲突堪称最残酷的较量。人们的态度与行为（无论友敌或未决者）终将决定冲突的走向。"

——加拿大武装部队《心理作战联合条令》

我曾栖居于半影之界。一个充满秘密与谎言的世界。一个不可言说之地。一个不容发问的场所。一个充斥着迟滞反应、阴谋诡计和欺诈的空间。江湖帮派小圈子在这里巩固自身。权谋之术在“必要性”的幌子下上演，同志们或在窃窃私语中被逐出局外，或在无声中被隔绝于圈内的边缘。唯有“适者”得以存续，其余者皆遭弃绝 —— 无论是挚友、爱人、抑或仇敌。

你会亲眼看着亲密伙伴的眼睛里闪烁着搜寻恰当措辞的惶恐，为绕开真相而迂回的话语，而同时，你自己也对他人做着同样的事。有时，你甚至连那样的眼神都看不到，一切都被伪装在阴暗的深刻中。你能窥见其中的运作机制，却无法言说所见。正如你以千万种方式信任对方，却无法吐露所知。

这就是提问即犯罪的地方。在这里，你被剥夺了发声的权利。在这里，真相无处容身。尤其是当你未被纳入“核心”、遭人排挤时，便只能栖身于秽语症般的臆测、否认、不安、挫败与偏执的维度上。

透过这层秘密与谎言的筛子，透过我们社会关系织锦上千疮百孔的破损，我们会迷失自我。我们会失去彼此。在诚实已然止息的地方，我们成为了自己的囚笼。

[image]

> “我们知道，保密行为的本质会侵蚀践行者的个性。对于所有形式的保密都是如此，从原始的秘密社团到密语隔间。后者是一种强化形式的保密，在许多方面类似于前者。它带有秘密社团的光环。它有入会仪式、誓言、深奥的“行话”、隔离区域，以及层层嵌套的秘密。取代暗语手势的，是徽章上的字母代号。这里有圈内人和圈外人。难怪密语隔间会产生意想不到的心理效应。”

— *1977*年*3*月的一份报告《中央情报局密语隔间批评》

【隔间 (Compartment): 指代一个高度机密的信息系统，信息被严格隔离，只有被明确授权的人才能访问。密语/码字，指代秘密任务或人员。】

难道我们认为国家在保密方面的专业程度，不如它对战争的精通吗？全世界每个国家的秘密部门工作人员，都对保密制度给守密者以及无权接触秘密者的心理带来的压力和影响有着第一手的经验。难道我们认为，在耗费千年磨砺刀刃之后它不知道该以哪个角度、切割哪块血肉才能得到最好的肉质吗？

构建秘密就是构建高墙，就是构建评判，就是将我们彼此分离，就是播撒不满、猜疑和偏执，就是隔离那些敢于直言现状者与可能倾听者。因此，国家又写下了心理战的新篇章。创造一个播种秘密的花园，实则是播撒权力与腐败的种子。

在其他时代以及在当下的某些地方，必要的秘密活动是需要宣誓的。国家处决人们，不仅因为他们采取行动，很多时候仅仅因为他们对一个从事反国家行动的组织宣誓了保密誓言。而在那些秘密组织中——例如斯温船长（Captain Swing）、卢德分子（Luddites）、莫莉·马奎尔斯（Molly Maguires）、爱尔兰共和军（IRA）—— 规则始终明晰。有流程、有仪式、有入门和除名，不仅针对战士，更涵盖他们的家族和社群。

负有责任的行动也许不是我们对抗国家的首选方式，但选择保密本身并非力量。这是一种无奈的必要，也是国家精心营造的一种存在状态，正如可追责性，这种状态同样契合其统治的需求。

在一个充满秘密与谎言的世界里，存在着一个影子的世界。影子是黑色的、冰冷的、扁平的。它们不会流血也不会哭泣。它们没有质感，没有色彩。它们拥有人类的轮廓，但缺乏灵魂。在这场影子的游行中，有一种虚假的强大。

当个体试图通过国家提供的半成形入门仪式来实现自我时，就是他们被去个性化的时候 ——这些仪式将人类所有本能（包括坦诚的本能）定为罪行。

[image]

在某种程度上，在缺乏真正的亲密和情感色彩的情况下，影子们彼此交融。

在一片黑暗的模仿中，在这种统一的逃避孤独和孤立的方式中，影子们合为一体。

形成一道对抗“他者”的高墙。

> 拉尔森与查斯坦（Larson and Chastain, 1990）发现，保守秘密的性格倾向，也被称为自我隐瞒，除了与身体和心理问题相关的压力因素（如创伤经历或缺乏社会支持）之外，还会导致直接的身体不适和抑郁。基于这些发现，拉尔森和查斯坦总结道：‘保密，无论所保守的秘密类型如何，都‘会付出代价，并起到内在压力源的作用’。针对成年人保密现象的研究和理论表明，保密所带来的身体、心理和社交劣势，可能是巨大的。

就其本质而言，保密将保守秘密者与被蒙在鼓里的人分离开来。保守秘密者就是看门人。他们必然需要对周围人的品质、可信赖性以及是否达到值得被吸纳的标准，做出判断和评估。保守秘密者及其对其他秘密持有者的筛选并非中立。而是充满着权力。如果我们真的相信权力必然导致腐败，我们就必须对我们的保密行为保持谨慎。

通常，由于我们的政治网络具有极强的非正式性、加之政治世界与社交世界的密切交融，我们对保密措施的使用意味着我们可能会对什么是机密、什么不是，谁是机密人士、谁不是感到困惑。又因为政治派系与社交团体和生活集体并存且交融，彼此之间存在大量的交叉，所以那些暗示保密的行为往往昭然若揭，再加上自我意识的驱使，这常常会演变成一种表演，一种权力的展示和人际偏好的表演，最终不过是一种粗糙的拉帮结派心态。

我们假装中立和严肃，但如果将我们的行为和流程与二十世纪初的波

兰无政府主义团体“革命复仇者”进行比较 —— 该组织的成员甚至被禁止在工作场所表达政治观点，以免危及组织的秘密活动 —— 也许他们会被指责为先锋主义，但他们也有值得我们学习的地方。

我们选择某个人作为秘密守护者，往往是因为此人具有吸引力、令人向往、有地位有声望、穿着得体、阅读正确的书籍、行为举止合宜、拥有某些人脉，以及因为他们是我们的朋友。我们也可以基于同样的理由而孤立他人：因为我们不再喜欢他们，不再与他们亲密，因为另有其他人更让人兴奋，因为其他人有更高的地位和声望，甚至仅仅因为我们中一些人善于操纵社交网络，擅长趋利的“站队”。

[image]

亲密团队模式具有重要的功能和优势，但不可否认也同时有其缺点。

其中之一就是缺乏个人政治问责制，以及大量松散关联的小团体 —— 这些团体的成员可能对其他团体中的个人没有亲近感或责任感，从而可能导致缺乏尊重的流程，隐秘的个人动态在暗中滋生，当人际或政治问题出现时，没有第三方调解的可能性来减轻权力滥用。

由于安全方面的考虑，当一个人被排斥时，这个人没有“圈外”的人可以倾诉和疏导，

这就会让他们陷入双重的孤立 —— 首先因为他们的政治观点和生活而被整个社会隔绝，现在又被这个本该是同志的团体所隔绝。

在激进主义圈层中盛行的亲密团队概念，比任何其他政治形态都更凸显个人与政治的复杂纠葛 —— 这是我们多数人难以应对的敏感议题。

秘密与谎言的代价高昂，它要求保守秘密者和被排除者（其中可能包括前保守秘密者）动用否认、分裂和解离等心理防御机制。我和多数人一样通常认为保密文化关乎安全：是对镇压的必要反应。但我也有一种感觉，它关乎不止于此。如果缺乏充分觉知，秘密本身可能已经在某种程度上变成了目的。

研究表明，保密对成年人的影响极具破坏性，会导致孤立感、抑郁和身体不适（无论守密者或非守密者皆然。守密者可能是看门人，但他们也是自己知识的囚徒）。在任何政治激进场域中，保密文化和帮派心态的负面影响都是显而易见的。

然而有趣的是，针对青少年的研究表明，保密在他们从儿童到成人、从依赖到自我实现的过渡中，可以是一个积极因素。如果我们将此视为对当代一些抵抗团体的隐喻，便能理解保密作为一种选择的意义。在这个剥夺我们的情感、自我掌控能力与生命意义的世界中，保密文化可能不仅仅代表着一种战术上的需要，更是一种心理上的需要。

正如青少年通过隐秘行为绕避权威者（父母、教师等）以实现个体化，从而开始彰显自身独特性与自主性一样，政治群体中的保密文化也有可能 —— 除了是对镇压的反应以及保护自己免受监视和行动的法律后果的需求之外 —— 是一种类似于青少年阶段的无意识过程。

> “……保密是青少年福祉和心理健康与社会发展中的重要机制……它独立地有助于青少年的心理社会福祉，并且似乎是青少年自主感的核心因素。”

当这些团体努力对抗国家、司法机构、企业工业界和军事霸权等压迫性权力机构，主张其个人和意识形态的自主权时；当他们努力“与他们的主要看护者 [国家以及家族、教育和规范化的社会结构] 保持距离，并脱离关系，在‘自我’和‘非自我’之间建立界限（Kaplan, 1987）”并“建立和巩固他们的自我调节和自我决定能力（例如，Allen et al., 1994; Larson et al., 1996; Steinberg and Silverberg, 1986）”的时候，这些政治圈子选择保密，不仅仅是作为一种反应，一种避免因攻击国家而被侦查和惩罚的手段，同时也是一种界定自身差异、创建独立派系的方式。

[image]

镇压有许多面孔，身体暴力和监禁威胁只是其中之一。极权体制的另一种压迫形式，是制度化的幼稚化与依赖性不断加深的进程。从最基本的需求开始 —— 即温饱出行自我教育等 —— 我们就已经沦为依赖者了，无论是三岁的孩子还是六七十岁的老人皆然。

我们鲜少能认识真实的自我，梦想与渴望永远无法自由绽放。这种生存状态导致人类陷入永恒的未成熟境地。

人类将不顾一切地争取自由、力量和自我实现。作为青少年，我们通过组建团体、入会仪式、制服和服装标志以及共同的标准、身份认同和创造独特的秘传知识来实现这一点 —— 亚文化。显而易见这种封闭隔离包含了固有的反动风险，就政治团体而言，除非我们想保持微小并复制那些阴险的权力结构，否则，我们最好能早点意识到这些结构和行为的心理影响。

生活在发展停滞的状态中，并不是在重新找回完整的人性。

[image]

“心理战（PSYOPS）的三个基本目标是：

1）削弱敌人或对手的意志，通过在其内部制造怀疑、异议、和不满，来降低士气和效率。

2）增强友好目标受众的情感认同。

3）争取未承诺的或摇摆不定受众群的支持与合作。”

—— 加拿大武装部队《心理作战联合条令》

所有保密文化都会遇到问题。如果它们关乎效能和安全，那么它们就需要不时地进行审视。即使是中央情报局也承认高度保密造成的心理和效能问题。一份报告甚至提出，保密实际上会导致不安全感和低效：非敏感信息与绝密信息一起被封存，从而导致行动失误、不满和不必要的权力博弈等问题。

当我们开始允许病态的保密文化滋生，那么，如果我们的目标是某种程度的人类健康、相互尊重和团结、自我（亦指更广义的同志集体）

实现和自主性，我们就需要不断警惕我们的动机以及我们对待彼此和整个世界的方式。

由于我们投身“激进主义”的方式非常非正式，有时甚至是偶然的，这种状态常缺乏充分的自觉、讨论、觉知或正式引导。无论在秘密圈子之内还是之外，都存在着一种人际关系紧张、偏执、归属稀缺性与排斥感、士气低落、孤立感或特权感、等级制度和个人不安全感的倾向。这可能是破坏性的，足以令人瘫痪。

[image]

我们需要问的第一个问题是：在任何其他世界中，这种保密的生活，本质上是这种与他人相处的方式，会是我们主动选择的吗？

如果是，缘由何在？

如果不是，那么我们如何才能最大限度地减少被强加的局面所造成的损害，并在这个过程中寻找到合理化依据？

我们想要一个什么样的世界？

我们现在正在创造的是什么样的世界？

如果我们在当下继续互相伤害，难道真以为未来某个解放时刻这一切会奇迹般地改变吗！？

今日，我无法言语。心悬于喉。颈部以上都已麻痹。我的喉咙。我的嘴巴。我的舌头。我的嘴唇。我的言语。我的思绪。交流已不复存在。诚实也已停止。取而代之的是眼神、暗示、猜测、狡黠的微笑、手势，是人们将另一些人拉到一边，远离那些可能被允许知晓或永远都要蒙在鼓里的旁观者。我永远无法确定自己是否理解了正在发生的事情，也无从查证。

混乱在蔓延。安全被搅乱并洗牌。没有逻辑可言。有些地方可以公开

交谈，但似乎并不比禁言之地更安全。而决定边界的人们，既无章法也无澄清。唯有偏执与迷茫。被排斥的恐惧，被接纳的庆幸。权力与自我交织。

每当我开口说话，都会感到一阵恐慌。每当我张开嘴巴，都能感觉到脸颊因恐惧而发烫。每一次在话语落下后闭上嘴巴，每一次打电话给某人，每一次按下电子邮件的发送键，我都能感觉到肾上腺素的飙升。就连最简单的表达也伴随着这种感受。甚至似乎如果没有这些感觉我就再也无法说出任何事。我的舌尖干涩，思绪纷乱，嘴唇僵硬。我半遮眼帘以便与你同步。这被称为模仿，它在社交排斥的情况下潜意识地发生，作为安抚或讨好排斥者的尝试。

每一次互动都沾染着法庭般的猜疑、自我意识和恐惧。每一段友谊都变成了一座监狱，我们隔墙相望。情感也在消逝。

[image]

我曾以为我们是反叛者。如今却成了站在操场边缘的少年，困惑为何无人再与我嬉戏。操场对面是我曾经身在其中的小圈子。一切一如既往。唯独我已不在其中。我在这里。在外围。在那些不久前还是我的朋友、爱人、同志的人所筑起的高墙的另一边。

因为我不再被视为合格者。因为我的爱人离开了我，友人亦弃我而去，因为我感到不得不离开共居的屋舍却无处可去，我身处一个陌生的地方，不是我长大的地方，说着我不懂的语言。更因我在重压之下有些崩溃，我不再被认为适合行动。

我被少数人秘密地、在我背后的谈话中评判了，没有经过任何正当程序，直到我追问才被告知。我认识那些迹象、眼神、那些暗语。只是它们不再指向我。曾经视作抗争必备的归属感，此刻却愈发像是一场表演。一场保密的奇观，其动机之一似乎是向他人展示他们被排斥的状态，以及那孔雀开屏般的“被接纳”。

突然间，在这个对一切都有见解的反叛者世界里，突然无人发声了：不问发生了什么，谁做了决定又为何如此，你身在何处，是否安好，是否另组团体，我们该如何应对？...... 提问本身被禁止了。

尽管有些人仍是“朋友”，但背叛的泥沼和异样的共谋在彼此间散发着恶臭，友谊无法跨越这道鸿沟。

我不想再成为某个圈子的一员。我只想再次被接纳。

这里没有团结感，没有亲近感。只有愤怒与无力。只有孤立和抑郁。只有精疲力竭。只有骄傲。只有挫败。

□

守密者的笑声带着秘密的狂妄，他们的身体因谎言而傲慢。他们的眼睛看向除了我之外的所有地方，而我这辈子，穿过监狱、穿过逮捕、穿过袭击、穿过暴动、穿过激烈的辩论，之后，我却第一次，没有了同志。

> 在研究中观察到，在实验过程中经历 被群体排斥 的人 感觉身体更冷 。当被要求评估房间温度时，他们报告的平均温度 比被群体接纳者更低 。当被要求从一系列食物和饮料中选择时，那些被排斥的人 请求更多的热食和热饮 ， 远远超过 被接纳者。

即使我身处秘密之中，即使我被接纳，我仍感到不适。这就像身处一个充满虐待的家庭中，家庭之外的每个人都是你不能透露任何重要事情的对象。在一个充满秘密与谎言的世界里，其他所有人都是“他者”。其他所有人都是未被纳入的、不被信任的、不受欢迎的、没有特权的人。其他所有人都是需要你畏惧的存在。

你与其他所有人被根本性地分离、解离。你的对话因那些未言明的、不可言说的内容而变得灰色沉重。你们彼此太亲近，但却又永远不够亲近，既被孤立，但又不够孤立。你生活在一个以匿名为特征的世界里，但又不够匿名，以至于你所守护的秘密、分享的隐情、以及你所推崇的同谋者所带来的影响，无法向你的“前”亲密朋友的“现”被排斥者隐藏。

与秘密圈层之外的人的交流不再自由，因此对秘密圈层的依赖循环愈

发加深。所有让你感到困扰的关于秘密或关于这个滥用权力的团体的问题，都无法被谈论，导致更深刻的孤立感 —— 除了那些同样守着秘密、却正是不安根源的同伴。

当你被这样隔绝于世，认定世人“皆不可信”时，偶尔会不禁自问：「我究竟在为谁而战？」

这是几个月来你第一次让我关掉手机，以便我们可以自由交谈，这份被接纳的感激之情竟令我作呕。

守秘时的我们经历着怎样的情绪？是好战的、羁绊的、封闭的、尴尬的、困惑的、强大的、被接纳的、特权的、坚韧的、偏执的、压抑的、亢奋的、危殆的、欺骗的、还是渴求的？我们如何应对所有这些感受？我们如何围绕着它们生活？我们如何对过这种生活带来的无数后果以及我们做出选择背后的潜意识原因保持警觉？与那些无需守密的人相处时，我们又该如何定位彼此间的关系？选择守密伙伴的依据何在？我们在守护的是什么秘密？以及我们何时仅仅是为了形式和快感，而不是出于必要性，而在坚持保密？

秘密的世界是情人专属的天地。它承载着亲密与共谋，交织着政治与私情。置身于这样的情人关系之外可能是一种折磨。尤其是当他们曾经也是你的情人时。处于这样的情人关系之内也可能是一种折磨。尤其当其他情人被排斥在外时。

我知道我终将遇到新的情人和其他的秘密。但我会尝试以不同的方式去面对。怀着对先驱者的敬意，怀着对成熟历程的尊重，在深刻认知彼此伤害之广度的同时，我们需要将隐秘性与人性相结合，并保持对内在与外在体系的持续警觉。

[image]

附言（实用建议）

我写《秘密与谎言》是在一年前。在那一年里，我完全退出了政治圈子，远离了我所认识和认同的所有人与事。我深思了引发《秘密与谎言》的处境和政治场景：反思我自己在其中扮演的角色，以及其他人扮演的角色。当然，我们都有权决定不再与某人合作，而且我们都必须学会在某个时刻从排斥者和被排斥者的角度来处理这个问题。所以，以下是关于在这种情况下可以做得更好的几点思考。

1.

当我和我的同志之间的关系开始瓦解时，我们确实定期进行过沟通，并尝试继续一起合作项目，只是不涉及高度“敏感”的项目。

通过这种方式，我们试图重建彼此的信任、信心和了解。

我推荐这种做法，尽管在本案例中它没有奏效。

2.

不要假定中立立场：如果你需要在情感复杂、涉及多方的困境中寻求建议，请思考所涉及的关系，以及你在做选择时对某些行为/反应（如操纵和/或剥削性的行为/反应）赋予了什么样的价值观和判断。

3.

在确保安全的前提下，尽可能坦诚地告知被排斥者其处境，并承认这种排斥带来的影响。

除非有非常充分的理由，否则应该告知被排斥者任何关于他们的讨论，或者更好的是，让他们在场，以便他们能够参与决策并在需要时提出质疑。

[image]

将某人排除在行动之外是很难的，如果继而又使其在充满安全隐患的处境中陷入孤立无援的境地，不仅对其本人的情感健康、并且对所有人的安全都构成不负责任的行为。

4.

如果被排斥的人是你，并且你觉得自己有必要就此进行沟通，包括弄清楚别人怎么看你、你的立场是什么，那么请商定可以和谁谈论这件事。

你可能需要主动一些，因为其他人可能感到尴尬、不确定是否可以谈论，或者选择逃避。

如果可能，安全地请一位来自附属亲密团队或另一位来自共同认可的圈子之外的可信赖人士来倾听。

虐待和权力滥用模式经常在封闭的团体中滋长 —— 例如每个人都熟悉的核心家庭。

5.

此外，与伴侣一起工作时要谨慎，或者至少要非常确定你们都能处理好相关问题。从长期安全角度出发，彼此间需谨慎行事。我们都认为亲密之人不会出卖自己，但历史上甚多残酷的镇压行动都在表明，人情世故变幻莫测 —— 昔日的至亲至爱为了逃避长期监禁，竟会出卖亲友。

当（如果）警察突然找上门来，把你单独拖进牢房，告诉你“某某某”说了你什么，或告密了什么，你过往对人性的认知将决定国家心理战对你的侵蚀程度。

如果你曾目睹战友在斗争的压力下崩溃，表现出令你费解且不安的行为反应，你又如何确信当警察以更私密的方式施加恐怖时，他们不会重蹈覆辙？

[image]

国家镇压旨在分化、压倒和摧毁我们—— 你我生命中有哪些纽带维系着战友间的紧密相连？

我们又如何处理彼此的弱点和局限性，又如何接纳彼此的优势？

想想看，你与谁在一起感觉亲密？基于什么理由？

6.

审慎地对待保密，要有分辨力：保密是真正必要的吗，还是关乎其他东西，比如权力和自我膨胀？

不要忽视权力动态：人们在特定时间可能处于较强或较弱的地位，如果有人看起来或感觉自己由于某种原因处于弱势地位，请尝试理解缘由并给予宽容。

7.

我们不是机器人：所谓的生活私域与政治公域并非总是那么容易分离，尤其是在基于亲密和非正式性的团体/圈子中。

但每个人都有差异 —— 有人需更包容情感波动，有人则需提升情绪管理能力。如果你自认是易受不安、嫉妒、骄傲等致命罪恶困扰的“情绪化之人”，就必须主动掌控情绪，在矛盾激化前化解危机。

如果你并非“情绪化之人”，也切勿否认他人可能存在这类特质 ——

否则诸多问题将被掩盖，日后终将爆发出来。

8.

我所经历的这类人际问题实则反抗斗争的一部分：它提供了一个创造/实验新型社会关系的机会，也是一个让我们近距离观察到社会体制如何通过我们的行为和动态在我们身上上演的机会。如果我们勇敢地看待所有这些事情，我们就能深化我们的反抗运动，更长久、更强有力地战斗。

祝好运，请照顾好自己和彼此，不要被捕！

[image]
[image]

了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image] 关键词	人际安全 心理安全 线人 诱捕
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；👹渗透者 ；□告密者（线人）
[image] 创建时间	2025年1月7日
[image] Description	反渗透和协作

不只有保护自己。因为您独自一人是无法实现安全的。只有当我们能够互相照护的时候，安全措施才能起效。

- Table of Contents

  本文分为3部分：
  当局有可能如何诱捕反抗者?
  举一个例子
  为什么是诱捕？
  如何摧毁一场运动
  重述统治阶级的这一镇压战略：
  下一步是什么
  如果政府间谍想要你做线人，怎么办
  1、我有义务与警察合作吗？
  2、如果我真的跟他们合作做了线人，他们会保护我的身份吗？
  3、如果我不告密，这些政府间谍能让我出庭作证吗？
  4、如果他们威胁要逮捕我，除非我答应通风报信，难道我都没有接触律师的权利吗？

5、当政府间谍试图让我当线人时，他们是否有义务给我他们声称提供的东西？
6、我可以给间谍提供虚假的信息吗，以便让他们不找我麻烦？
7、我难道不能向他们提供毫无价值或毫无意义的信息吗？
8、政府间谍在接近我之前是不是已经掌握了我的情况？
9、他们接近我的几率有多大？有多少线人，这些线人对政府间谍的活动有多重要？
10、如果政府间谍已经和我谈过，我因为害怕而同意帮助他们，怎么办？
11、如果有人找我做线人，我应该怎么做？
此人可能是线人吗？如何判断？—— 十点清单
1.
2.
3.
4.
5.
6.
7.
8.
9.
1.
2.
3.
4.

[image]

渗透者的工作并非只有监视 ……

本文将继续详细解释渗透问题。

本文分为3部分：

1. 当局有可能如何诱捕反抗者?

1. 如果政府间谍想要你做线人，怎么办?

1. 此人是线人吗？如何判断？—— 十点清单。

[image]

当局有可能如何诱捕反抗者?

首先来回顾一下最基本的知识。

🚫

不要与您没有足够认识或者没有信任过较长时间的人讨论行动相关的具体细节。

不要仅仅因为您认识的其他人信任某个人、或者某个人处于圈子内“具有影响力的位置”就选择相信他们。

不要让别人说服您采取您本来有顾虑或不准备采取的战术。

要意识到，您说的任何话都可能在不久之后返回来困扰您，即使您当时不是故意说出的。

始终听从自己的直觉；如果有人看起来咄咄逼人或太急于“帮助/插手”您的事务，应该花些时间考虑一下情况。思考您周围人的动机 —— 合理吗？了解您的战友的家庭和朋友。

不是怀疑！而是了解。知晓。通过沟通。保持亲密。

这些做法都是明智的，但还不够；我们肯定不能只从个人角度考虑安全问题。即使100人中有99人能够避免被陷害，但当挑衅者设法诱捕仅剩的那个人时，我们所有人最终还是要付出代价。

我们需要一种安全文化，尽可能保护其他所有人的一种文化 —— 包括激进空间中的弱势和边缘参与者，他们可能是政府间谍特别感兴趣的目标。顺便说，如果您是组织者，尽可能少的等级落差/尽可能少的产生“边缘”，应当作为安全措施中的基础部分。

除了关注您自己，也要关注可能使您处于危险之中的其他人。

[image]

返回 - 练习：[image]S01E03-T1 周围是谁？可视化人际关系图谱

返回 - 练习：[image]S01E03-T2 绘制行为者关系图谱

例如，想象一下，您参加了一个演讲，听众中的一个人不断提出疯狂的问题，要求人们升级(更暴力的)战术。这个人有可能是渗透者在实施挑衅；也有可能不是渗透者，而是一个头脑发热的糊涂虫，而这样没头脑的人可能成为对政府间谍来说非常有吸引力的目标。

没头脑的人通常会被避开，但要注意孤立感只会让他们更容易受到政府间谍的拉拢。

“去他妈的这那些广场—— 跟着我，我们真的能有所作为！”、“我们只是还没有枪！其他一切都是无意义的”，等等，你一定听到过类似的话，这是很可疑的迹象。遇到这种情况时，应该派出一名在此事中没有任何损失的人在一个低压力的环境中接近那个可疑的人，并强调适当的安全文化的重要性，描述一个人如此粗心大意地说话会使自己和他人面临的风险，并敦促此人谨慎地相信任何招募他/她参与非法活动的人。像这样十分钟的谈话就可能会在以后的日子里省去多年的心痛和入狱的麻烦。

[image]

举一个例子

不久前，联邦调查局似乎在专注于追捕有成就的无政府主义者。

Marius Mason 和 Daniel McGowan 在长期参与反抗行动后被逮捕。国家维稳机构将这些活动家作为目标并不令人惊讶：他们勇敢地威胁着国家所建立的不平等和不公正的统治系统。

但此案中需要注意的是，首先被政府间谍瞄准的并不是这两位资深活动家，而是他们身边那些没有实际进行过任何行动的、缺乏经验的年轻队友。在此案中就是埃里克·麦克戴维（Eric McDavid）。当局通过对麦克戴维的诱捕 —— 利用一名女性渗透者，借助麦克戴维对这个女孩的兴趣，以操纵他讨论敏感的行动。

色诱，是秘密行动的标准手段之一。

政府间谍在2008年共和党全国代表大会期间加强了这种新战术，在这次大会上，联邦调查局的线人布兰登·达比和安德鲁·达斯特陷害活动家大卫·麦凯、布拉德利·克劳德和马修·德帕尔马，指控他们在两起事件中拥有自制燃烧弹。值得注意的是，在全国代表大会的抗议活动中，唯一出现的自制燃烧弹正是用来诱捕这些年轻人的 —— 联邦调查局不是在应对威胁，而是在制造威胁。

2012年初，联邦调查局的这种做法已经进入了高潮。五一节前夕，五名年轻人在克利夫兰被指控犯有“恐怖主义罪”，因为一名联邦调查局的渗透者显然引导他们计划炸毁一座桥梁，如果实现，也是有史以来无政府主义者实施的唯一此类爆炸事件。在芝加哥举行的抵制北约峰会的抗议活动中，三名年轻人被逮捕并被指控犯有“恐怖主义阴谋罪”，这又一次涉及到数百英里内唯一的燃烧瓶 —— 由至少两名联邦调查局的线人设置。

[image]

抵制北约峰会的抗议活动中，卧底线人“Mo”和“Gloves”（又名“Nadiya”）

这些诱捕案所针对的目标都不是长期的反抗行动组织者。他们被指控的罪行都不代表无政府主义者在过去十年中实际使用的战术。纯属👎栽赃。所有的案件都建立在政府间谍的线人制造阴谋的努力上。所有的逮捕行动都发生在大规模反抗行动的动员之前，使当局能够为其镇压抗议活动的行为辩护，将反抗者说成“恐怖分子”。在所有这些案件

中，被告都在针对他们的法律文件中被描述为“无政府主义者”，为当局对无政府主义的定罪创造了先例。

为什么是诱捕？

为什么政府间谍专注于诱捕没有经验的年轻人，而不是去追捕经验丰富的资深活动家？为什么他们现在要加强这种战术？

首先，有经验的活动家更难抓捕。政府间谍是为了钱而工作的，与活动家截然不同，间谍往往不会出于激情或信念去工作。他们的报告往往读起来像二流的家庭作业，即使他们真正破坏了人们的生活。这些间谍根据成功的案件而获得资金和晋升，他们甚至有“抓人指标”，所以他们有动力去陷害别人；但为什么不要去找有挑战性的目标？为什么选择最边缘化、最脆弱、最孤立的人呢？如果目标只是为了陷害某人，那么目标是谁并不重要。

同样，无政府主义者实际使用的战术可能比渗透者推动的战术更受公众欢迎。例如，打碎银行窗户可能是非法的，但它越来越被理解为一种有意义的政治声明；而对当局来说，围绕碎玻璃很难建立一个令人信服的所谓“恐怖主义”案件。

[image]

知名的活动家不仅有成熟的安全性防卫经验和技能，而且拥有更广泛的公众支持网络。

联邦调查局威胁要对丹尼尔·麦高恩判处强制性无期徒刑和335年监禁；广泛的公众支持使他能够获得一个好的律师，而检方不得不接受认罪协议，判处7年监禁，否则检方就要承认从事非法窃听活动。

而通过强迫失踪对失联的年轻人下手，就大大减少了公众将被动员起来支持被捕者的资源。

如果重点是 建立先例，将反抗行动定为犯罪，同时产生最小的反作用

，那么对于当局来说，通过挑衅者的手段制造虚构的 “恐怖” 案件比调查实际的反抗行动更加容易。

最重要的是，这种主动创造威胁的做法使政府间谍能够为媒体宣传活动做好准备 —— 如果一个抗议活动即将发生，当局预计将使用残酷的武力镇压，那么能够提前将故事编成 “对暴力犯罪分子的必要的、有分寸的反应”，就会有帮助。

这也在活动家之间播下了不信任的种子，并恐吓新来者和犹豫不决的成员脱离队伍—— 在哈萨克斯坦发生的事就是如此。这里的长期计划，估计是由间谍机构的领导层而不是普通的特工人员编排的，不仅仅是为了陷害几个不幸的被捕者，重要的是为了束缚整个反资本主义运动。

[image]

如何摧毁一场运动

正如您在过往很多镇压案例中都能看到的那样，政府间谍的镇压操作往往是在反抗运动开始分裂和消退、战略目标的群众支持基础出现减少时，开始入手并认真进行的。在我们这个超媒介化的时代，反抗运动的生命周期过得越来越快；占领运动在2011年11月达到顶峰时已经开始放缓，就在那个时候使当局更有胆量巩固其控制并进行报复式镇压。

随着无政府主义价值观和实践在抗议运动中变得越来越重要，全世界的统治阶级都在急于使无政府主义者失去行动能力并使其丧失合法性。然即便在这种情况下，承认仅仅因为“无政府主义”政治立场而把人作为目标仍然是不够完整的 —— 镇压者需要把话说圆，以免引起公愤。同样，如果没有将被作为镇压目标的个人描述为与该运动的其他成员 ‘格格不入’ 的叙述，统治阶级也不敢发起镇压，即使这种镇压是为了摧毁整个运动本身。

[image]

换句话说，当您真正经营一个直接行动的亲密团队时，团队中的每一个人都必需获得足够充分的发言权和权益，每个人都是“亲人”，尽可

能不要有边缘化的现象，不仅仅是平等问题，更是免于发生诱捕策反的重要安全性措施。

对政府间谍来说，幸运的是，“占领”运动中的一些“非暴力”倡导者很乐意提供这种叙述，不承认所有没能肯定其狭隘战术框架的人。当叙事作为战术时，有着非常微妙的但可能很严重的后果性问题。像克里斯·赫奇斯（Chris Hedges）这样的记者更进一步，把“黑群行动”说成是“一类人”，而不是一种战术 —— 尽管连《芝加哥太阳报》都明白其中的区别。赫奇斯带头将那些积极捍卫自己免受国家镇压的反抗者归入了这一捏造的政治类别 —— 实际上是将他们指定为合法镇压目标了。不久之后，诱捕案接踵而至，这并非巧合。

[image]

> “我们指控的人不是和平抗议者，他们是国内恐怖分子”，州检察官安妮塔·阿尔瓦雷斯说，“我们今天提出的指控并不表明抗议运动已经成为目标。”

当局迅速采取了这种叙述方式。在福克斯新闻推进联邦调查局议程的文章中，您可以看到当局在鹦鹉学舌—— 声称“他们[被捕者]利用占领运动作为幌子，但有自己的暴力议程”—— 以便将“黑群行动”诬陷为“本土的恐怖组织”。文章还将克利夫兰的被捕者描述为参与黑群行动”的无政府主义者”，但并没有任何证据表明他们中的任何一个人曾经参加过“黑群行动”。

这里的目标显然是将一种活动形式—— 匿名行动、保护自己免受警察的攻击—— 与‘一种人’联系起来：恐怖分子、恶人、怪物。这是当局的一个高度优先事项：他们能够更快地粉碎“占领”运动，至少相对于其数量而言，在人们不采取匿名行动和自我保护的城市，“占领奥克兰”与其他“占领”团体相比，寿命更长。在克里斯·赫奇斯和其他人的勾结之下，政府间谍和企业媒体的目的是确保当人们看到拒绝向强制性权威低头的蒙面人群时，他们不会想到“为自己站出来是件好事”，而想到“哦不…… 一群恐怖主义炸弹客”。

不论是今年初的哈萨克斯坦、还是去年的白俄罗斯、俄罗斯、哥伦比亚等举世瞩目的抗议运动中，您都能看到统治阶级采取这种分化孤立进而一举镇压的手段。哈萨克斯坦尤为明显，也是为什么我们连续多次更新以分析这些手段。

重述统治阶级的这一镇压战略：

- 通过孤立最具战斗力的参与者来分化和征服整个运动，对外围的脆弱目标进行阶段性的诱捕；
- 利用这些逮捕使所有的人都失去合法性，除了最温顺的、对统治阶级毫无伤害的那些人；并为不断增加的警察暴力提供理由。

在下面对哈萨克斯坦的分析中特别强调了这点 —— 要知道，全世界的统治阶级都擅长这样做：

[image]

下一步是什么

几十年来，各种反抗运动都在通过实践安全文化来抵御警察的监视和渗透。这使警察对有经验的活动家的行动效果降到了最低。然而，它不能总是保护那些刚加入直接行动或行动主义的人，他们还没有时间内化复杂的安全性习惯和做法，而这些人正是政府间谍诱捕战略的目标。

行动者团体已经开始呼吁建立一种集体安全文化，甚至可以保护新来者免受渗透者的影响。然而，在一个社会广泛发酵的时代，即使这样也不足以挫败政府间谍：您不可能期待做到接触并保护我们社会中每一个绝望、愤怒、脆弱的人。统治阶级只需要找到一个易受影响的年轻人，无论多么边缘，就可以推进他们的诱捕镇压战略。那些人是没有人性的赏金猎人：他们不吝于利用任何弱点、任何需要、任何心理健康问题。

如果我们要保护下一代的年轻行动者免受这些掠夺者的伤害，我们唯一的希望就是动员民众反对当局的诱捕战术。这并不容易，但没有更好的选择。

不要停止发言、组织和斗争—— 这不会阻止统治阶级压制我们或诱捕活动家；而我们的退缩只会让统治阶级更加胆大妄为：我们只能通过增加反击的力量来保护自己，而不是通过退缩，不是通过隐藏，更不是通过自我审查。

良好的进攻才是最好的防御。只要这个罪恶的体制不稳定—— 直到它崩溃—— 就始终会有压迫。反抗者必需迎战它。

[image]

如果政府间谍想要你做线人，怎么办

政府间谍接近你。也许他们只是随口问了几个问题；也许他们建议你跟他们做一个交易。他们可能会告诉你，他们试图 “帮助” 你；他们可能会告诉你，你现在有很多“麻烦”，除非你与他们合作，否则情况只会越来越糟；他们还可能会告诉你，他们需要你的帮助来防止一些可怕的事发生 …… 但无论他们说什么，都不要相信；你无法确定他们的真正目的是什么，也无法知道他们究竟想了解什么。

无论您是否已经被拉去喝茶了，或者您只是想为这种可能性做好准备，以下这些常见问题是您需要了解的最基本问题。非常建议您与您本地的法律学者联系以获得更多的观点。

不论是中国国安局、联邦调查局、克格勃、还是东德的史塔西，他们的行动都依赖于那些出于胆怯和自身利益而愿意充当告密者（线人）的人群。所谓的 “禁毒战争” 和 “反恐战争” 都是依靠线人的告密，使监狱里充满了数百万的囚犯。现在统治阶级正在恐吓和诱捕比以往更多的人，其明确目的是最大范围地压制异议。我们必须站出来反对这些恶棍。

1、我有义务与警察合作吗？

不，您不需要回答任何问题，也不需要向当局提供您的信息。

您和其他人都没有协助警方破案的法律义务。

法律上不要求您合作。

2、如果我真的跟他们合作做了线人，他们会保护我的身份吗？

尽管政府当局经常将线人称为“机密线人”或“机密人源”，但检察官可能有义务在法庭上披露你的身份，特别是如果你是签发逮捕令的核心人物、或者如果你在被告被指控的任何事件现场的话。

辩方也可以强迫你在公开法庭上作证。

一般来说，只有当线人对政府间谍和检察官持续可利用的情况下，当局才会关心保护线人的身份。

3、如果我不告密，这些政府间谍能让我出庭作证吗？

如果检察官或执法官员相信您持有相关信息，您可能就会被传唤作证。

您有可能避免这种情况的最佳机会是从一开始就拒绝与他们交谈。

这样，如果他们以后再来找你，其他人就有充分的理由相信你，并支持你继续抵制国家的压力。

您最强大和最安全的权利是从一开始就保持沉默的权利。

[image]

返回：[image]关于渗透 …… 一些基本须知

4、如果他们威胁要逮捕我，除非我答应通风报信，难道我都没有接触律师的权利吗？

虽然这可能取决于管辖权，但答案一般是否定的。

如果您被逮捕，您有权利获得律师，但是执法指南给予官员非常广泛的自由裁量权，当权者完全可以借此逼迫您提供信息。他们可能永远不会正式逮捕您，只是拘留您并胁迫您。

5、当政府间谍试图让我当线人时，他们是否有义务给我他们声称提供的东西？

这是一个灰色地带。

政府间谍可能会向正式的线人提供一份书面协议，据说可以像合同一样强制执行—— 但是，在这场谈判中，间谍们显然是更有实力的一方，如果他们不贯彻执行，也不会有任何损失。

警察和间谍经常保持着一个不在册的线人网络，线人的证词不会在法庭上使用，而是提供线索和有用的信息来帮助调查。

许多线人认为他们自己可以因为告密出卖他人而脱罪，后来才知道，他们仍然会面临指控，虽然可能较轻。

简言：间谍和警察关心的是全面镇压反抗社区和破坏社会运动，而不是保护线人。

6、我可以给间谍提供虚假的信息吗，以便让他们不找我麻烦？

大多数国家的法律都有规定，故意误导或欺骗警察和官员，包括执法部门，是一项罪行。

政府间谍在没有其他证据的情况下，利用这一法律就可以起诉他们怀疑的任何人。

[image]

请记住，如果执法部门正在寻找您做线人，他们很有可能还没有任何可以针对您的案子。不要给他们一个针对您的案子。

7、我难道不能向他们提供毫无价值或毫无意义的信息吗？

当政府间谍接触到您时，最好保持沉默，不合作，然后尽快与律师交谈。

您自己可能认为“无关紧要”的信息，您却不知道它对一个完全不同的案件至关重要；它可能牵涉到您无意伤害的人，或者给间谍一个真正骚扰您的理由。

如果您向他们提供关于任何人的信息，无论您认为这些信息多么无害，您都会增加他们试图恐吓和审讯这个人以及其他人的可能性——而且这些间谍绝对会回来继续试图从您那里了解更多的信息。因为您被认为是一个容易被利用的 软柿子 。

不要错误地认为您可以通过谈话来控制局势。您不可能知道间谍们询问的实际目的是什么，或者他们接近您的具体战术是什么。您唯一能控制的就是拒绝与他们交谈。

8、政府间谍在接近我之前是不是已经掌握了我的情况？

一般来说，是的。

以美国为例，联邦调查局特工可以进行所谓的“评估”。这个流程不需要任何搜查令或上级的批准，而且它可以像全面调查一样具有绝对的侵略性。

根据他们的指导方针，这种评估可以用来“寻求信息，以确定潜在的人类来源[即线人]，评估个人作为人类来源的合适性、可信度或价值，验证人类来源，或维护线人的掩护或可信度，潜在线人可能会提供或获得与违反联邦法律的犯罪活动、对国家安全的威胁、或与外国情报有关的信息。”

中国在这方面就更“自由”了，您无需质疑。

换句话说，政府间谍可以自由地接近您，说任何他们想说的话。

9、他们接近我的几率有多大？有多少线人，这些线人对政府间谍的活动有多重要？

数字时代让很多人误会了人工情报的重要性。

事实上，全世界的执法工作都依然高度依赖线人。以美国为例（绝对的数字高科技强国），仅仅是联邦调查局就为单一维稳计划维持着一个由大约15000名线人组成的网络。

自2001年9月11日以来，几乎所有与所谓的恐怖主义有关的重大起诉都涉及以政府线人为中心的刺杀行动；在涉及线人的恐怖主义起诉中至少有416名被告。

[image]

虽然不可能确定任何特定的个人被接触成为线人的机会究竟是多少，但可以合理地假设，只要政府间谍看到有机会收集情报或破坏您的组织，就肯定会接触和渗透您的社区成员。

10、如果政府间谍已经和我谈过，我因为害怕而同意帮助

他们，怎么办？

您没有义务合作。

您可以在任何时候援引您的权利来保持沉默。

如果您已经与执法部门交谈过，请立即寻求律师的帮助。

您还需要对您生活中的每一个人诚实地讲述您与政府间谍的谈话。如果您落入了间谍善于设置的陷阱之一，您应该对此完全诚实和透明，并完整地叙述您的遭遇。这是值得您的同伴信任的唯一方法，对您的行为负责，并使您有可能在需要时获得他人的支持。

即使您不泄露任何信息，您也应该向整个社区报告您与政府间谍的任何互动。

您不需要对您被间谍盯上的事情保密，盯上您的人已经知道了这件事了。由他们说出去肯定没有您自己坦诚说出来，更能帮助您的队友。让间谍的活动引起广大公众的注意，可以阻止间谍继续骚扰您的其他队友。这也使人们能够组织起来，相互支持。

11、如果有人找我做线人，我应该怎么做？

请记住这四点；

- 不合作是保护我们的社区和运动免受国家镇压的最佳方式。
- 如果他们找您告密，即便他们手里有您的案子，他们的案子也很可能很弱。
- 您不一定要合作。您有权保持沉默。

- 尽快联系律师。

> 我将死去，但这是我为死神所做的一切。
>
> 我不受他们的约束。
>
> 我不会告诉他们我朋友的行踪，
>
> 也不会说我的对手。
>
> 尽管他们向我承诺了很多，
>
> 我也绝对不会给他们画出通往任何人家门的路线。
>
> 我是活人国度里的间谍吗？
>
> 把人交给死神？
>
> 兄弟，我们城市的密码和计划
>
> 在我这里是绝对安全的；永远不会通过我令你被他们征服。
>
> —— 埃德娜·圣文森特·米莱，“凭良心的拒绝者”

[image]

此人可能是线人吗？如何判断？—— 十点清单

一群曾被线人挑衅者直接伤害过的人，根据个人经验以及其他活动家

的经验、和已经公开的线人挑衅者的信息，整理出了这份清单。我们希望您能从他人的前车之鉴中吸取教训，以便在这类人能够伤害您之前就加以制止。

以下是十个警告信号。

1.

感觉有些“不对劲”。这类人身上的某些东西不符合要求。他们关于自己的活动史或生活史的故事，并不真实。在这一点上，您需要进行一些 [image]背景调查 。

如果您只是等待所有其他迹象，可能就太晚了。

最明显的原因是，当某人出现在一个活跃的活动家社区，而在此之前，他们似乎并不存在。这应该是一个直接的危险信号。

2.

尽管一些成员有疑虑，但这个可疑的人很快就上升到了领导地位。

此人热切地在媒体上为自己的行动邀功，并开始宣传自己。

他/她努力成为该组织的“代言人”之一，显然想为该组织露脸，试图用该组织的名称、形象和身份来“塑造”自己的身份。

他/她喜欢被人拍照，即使是在从事敏感的活动时。

3.

他/她拍摄不应该被拍摄的敏感行动、会议和人物。

他/她将敏感行动和会议的照片发布在 Facebook 等社交媒体网站上，甚至未经其他活动家允许就给他们贴上了标签（实际上是为执法部门的监视提供便利）。

4.

他/她是个骗子。他/她有缺乏道德的迹象，对团体的其他成员缺乏透明度。

5.

他/她向不应该信任的人鼓吹高风险的非法行动，却声称“了解”安全文化的重要性。

他/她诱导他人采取暴力行动，例如告诉他们需要成为 “战士”。

经过思考就能发现， 此类可疑者建议的非法行动往往没有真正的目的，不会以任何有意义的方式推进反抗团体的战略目标 。这类可疑者通常对成为 “战士” 的意义有非常扭曲的认识。

他/她在社区中默默地寻找内部裂痕，并加以利用。他/她对团体和个人的虐待有一个循环：一个蜜月期，然后是操纵性的虐待行为，接着是道歉和承诺做得更好。然后循环往复。

6.

他/她总是有保释金和零花钱，但要么没有真正的工作，要么没有报酬很高的工作。

他/她可能暗示可以获得信托基金或类似的资源，但这需要核实。

他/她有经济自由，可以参加任何会引起媒体关注的行动，或任何可能涉及非法活动的地下行动。

7.

他/她被发现在身份、家庭、背景、种族或民族等真正严重的事情上撒谎。

8.

他/她有逮捕令，但不怕宣布和鼓吹非法行动，此类人使用自己的真实姓名，公开宣传自己的行踪，只要在非法行动中拍照或录像，这类人往往就会在画面中。

当被抓到时，这类人总是能获得保释并被释放，有时甚至在指控非常严重的情况下也能以自认身份被释放。这种情况经常发生。然后，这个人又回到敏感的行动主义会议中，拍照并发布照片。

这类人与警察之间有一个“抓捕—释放”的循环。

这类人可能有很早出狱的历史，然后直接去参加政治会议，有时是这类人私下声称讨厌的团体，或作为正常假释条件而被禁止的政治会议。

9.

您发现只提供给疑似线人的有价值的信息从执法者那里流出。

为了确保这一点，信息必须是明确无误的，并且是面对面的，一对一的，没有任何监视的可能性（例如，在田野中对线人耳语 [image]户外无设备对话 ）。

10.

完全承认："我的名字是______，我受雇于[某机构]来渗透[某组织]"。完全承认自己是线人和/或挑衅者身份，可能包括线人挑衅者因其工作而获得的细节：或者是他们得到的金钱数额，或者是他们得到的从监狱释放或避免因特定罪行被起诉的交易。

在某些情况下，交易包括未来在雇用他们的警察部门或情报机构中的职位。

如果上述符合其他标准，就应该假设他们告诉您的是事实，即使他们患有精神病。

虽然精神病患者不能成为可靠的线人，但他们可以成为优秀的挑衅者，而且当警察和间谍部门否认此人被雇为挑衅者时，他们的不稳定历史可以被作为证据引用。

[image]

如果一个人符合上述第1至～3点以外的任何标准，您就不应该和此人合作。希望上述第一点以外的所有内容都不重要，因为在第一个警示信号出现后，您就应该已经和这个人断绝关系了。

[image]

无论我们是否能证明某人是渗透者，如果此人表现出这里所描述的任何有问题的行为，他们首先就不应该参与任何敏感事件。

即使他们还不是渗透者，也有理由相信这样的人很可能在审讯中被策反或招供。

这里有一些其他需要注意的警示信号。

1.

在敏感会议和行动之外、在日常行为层面，可疑的人是否在伤害自己的同伴？

或者，他们是否试图与团体中的多个成年人（或其中一个领导者）上床？

性自由绝不是滥交。

间谍和警察经常雇佣被释放的流氓渗透活动家社区，于是观察某些人的行为举止，可能会有用 —— 对于真正的反抗者来说，其修养和价值观决策应该可以反应其声称的政治信仰。

[image]

返回：[image]为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力

[image] 女权主义性解放亲密关系的立场声明

2.

在最近收集到的经验中，一个符合上述十个标准中的九个的渗透者（包括第十个标准：向其他活动家承认他自己是线人），从未被执法部门定罪。相反，这类人在一系列活动家社区被释放，造成了破坏和毁灭。这样的案例可能并不罕见，他们中的一些人可能就在您的 Facebook 朋友名单上。

3.

当谈到线人挑衅者和直接行动的棘手问题时，问题的关键并不在于暴力或非暴力是否可取，而是，在于某人是否违反了其亲密团队的共识，未经队友同意就将其团队置于危险之中。

指责 “暴力总是挑衅者的杰作” 是不负责任的；

相反，挑衅者的出发点是煽动对参与者不利或孤立的暴力。

这里有一个例子。

除第九和第十条外，符合上述所有标准的人出现在一次公共游行中。这次游行被计划为一次和平的、合法的活动。也许不是这个团体的所有行动都是和平和合法的，但对于这个事件来说，这就是商定的战术。媒体对这一事件进行了报道，人们使用自己的真实姓名，老人和儿童也参与其中。

而挑衅者花了几个月的时间来讨好这个行动团体，每次行动都会出现，抢着埋单，帮人们安排乘车，说团队成员想听的任何话，甚至给他们买毒品。

但是，一旦游行开始，摄像机开始拍摄，这个挑衅者就开始不顾他的团体的安全或共识。此人不惜一切代价转移人群的情绪，煽动和鼓励高昂的情绪。

情况很紧张，挑衅者尽其所能地鼓励破坏纪律和违反先前商定的条件。突然间，他用一个小而重要的行动，比如说破坏财产或对个人使用暴力，为突然升级提供了引爆点。

然后， 当其他人纷纷效仿，在摄像机前爆发出非法和危险的行动时，挑衅者又消失在人群中，他的任务完成了。

此人现在已经把脆弱的和毫无准备的社区成员置于直接的危险之中，让人们处理挑衅者的行动的后果，而他自己却再次逍遥法外。

在 YouTube 上查看行动视频。有些人拍摄了自己的违法行动。一些视频包括这个闪光点时刻。注意是谁一次又一次地这样做。注意是谁因这些事情被捕，谁没有被捕，谁坐了牢，谁没有坐牢。

4.

经验丰富的间谍可能很难被发现。可能多数 渗透者 不是受过训练的间谍。很多告密者（线人） 是前罪犯，如果他们只是去参加会议和倾听，或者去参加会议和行动并进行破坏，他们就会得到一笔交易/赏金。

根据我们的经验，有少数但很重要的案件，有无辜者在怀疑中被误判。在很久以前影响到许多人的一个案例中，这种误认造成了毁灭性的后果。

这个错误是由于犯错误的人缺乏证据和经验，缺乏评估情况的可靠标准 。

通过提供这份清单，我们旨在帮助您提高在这些情况下识别和优先处理真相的能力。当一件事是事实的时候，它就不是 “草木皆兵”。

有很多关于安全文化的指南和文章。但是，仅仅因为一个团体发布了关于安全文化必要性的链接或声明，并不意味着这个团体中的每个人都在关注和正确实践安全文化。

希望这个检查表能成为一个有益的补充。

要安全，要有效，并相信您的直觉！

[image]
[image]

不放弃，不出卖：关于酷刑和证词

[image] 关键词	人际安全 团队 安全文化 审讯心理学 线人 诱供
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；□告密者（线人） ；[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09 ；🎀人际安全&关系结构革命-RelationshipsRevolution
[image] 创建时间	2025年1月8日
[image] Description	反渗透和协作；心理安全

本文署名作者“菲尔·库兹涅佐夫”已被确认为无政府共产主义者战斗组织**БОАК**创始人之一德米特里·彼得罗夫的化名。他于**2023**年**4**月**19**日在巴赫穆特战役中阵亡。 在这里看到 我们曾经对他的介绍，以及 一个纪录片 。

俄罗斯联邦安全局（**FSB**）前身是克格勃，对酷刑和各种间谍活动极为擅长。

- Table of Contents
原则从何而来？
1.
2.
3.
每况愈下的局面
革命者的经验
如何抵抗酷刑？
面对出卖，纠问式应对方式错在哪里？

杜波夫斯基案
再说几句
结论

[image]

自2017年以来，我们所处的这场运动遭受了前所未有的残暴镇压，范围和强度都达到了历史之最。其中最显著的特征就是俄罗斯联邦安全局（**FSB**）对酷刑的大规模使用。

以往，俄罗斯、乌克兰和白俄罗斯的无政府主义者遭受殴打和酷刑的案例，大多属于孤立事件。我们曾听闻激进的伊斯兰主义者和法西斯分子遭受了残酷的折磨，有些人可能还记得针对共产主义者和无政府主义者的"敖德萨案"。但是，"抽象地知道"是一回事，"亲身经历"则完全是另一回事。

酷刑导致许多人在落入特工部门手中后， 被迫指证自己的同志，跟镇压机器合作 。

俄罗斯无政府主义运动当前的危机，并不仅仅是旧有分裂和残酷镇压的结果。也许我们面临的更大挑战，是源于酷刑、泄密、以及背叛，所带来的道德困境，而我们至今仍未能充分应对。

我们该如何评价这种在被审讯过程中许多人背叛同伴的局面？酷刑可以成为辩解的理由吗？ 当运动中广受欢迎的成员，比如"网络"案中的伊戈尔·希什金（Igor Shishkin），最终也被联邦安全局击垮，成为了叛徒，这种情况下我们该怎么办？

这些问题不容回避。因为归根结底，它们引出了一个核心问题，即：当代的无政府主义运动是否还具有实际意义？它的存在是否还有价值？

酷刑和背叛的问题是近年来无政府主义运动中最重要的伦理困境。不解决它，我们就无法继续向前。

在无政府主义圈子里，可以听到的评判光谱始终在两种极端立场间摇摆，一种认为 ："任何人在酷刑下所做出的口供都不应被追究责任"、另一种则认为 "无论在任何情况下，向敌人提供情报都是不可接受的。任何这样做的人都是叛徒，是告密者，是线人"。

剧透一下：真相绝非是两者之间的"中间地带"。它更接近第二种主张，但并非完全等同。

让我们来仔细探讨一下。

[image]

原则从何而来？

我们从小就被教导"告密是不可接受的"。但这是为什么呢？

尤其是在面对酷刑时，如果仅从个人的角度来看，向施刑者提供他们想要的东西，以换取停止痛苦，无疑是最容易的选择。

然而，我们有几个理由说明这样做是不可接受的。

1.

最低限度是：当人们开始集体参与可能招致国家镇压的行动时，他们就已经期待了共同的秘密能得到保守。泄露这些秘密就是对这种信任的背叛这毫无疑问。如果事先知道在危急关头，同伴会把一切都告诉警察，那不难想象几乎没有人愿意冒这样的风险。

2.

但更强有力的理由或许是另一个：向敌人提供信息，实际上会毁掉其他人的生活。这些人很可能对你来说并非陌生人，你对他们有所了

解、有过深刻的交集。而由于你的行为，他们也将面临酷刑和多年的监禁。

3.

显然，这些论点同样具有相对性。事实上，如同任何道德准则一样，“不出卖同伴”的原则无法完全被“理性化”。但是，集体的传统、文化和经验告诉我们，这个原则是正确的。用克鲁泡特金的话来说，这是我们的“道德感”在指引我们。

同样基于此，我们将集体的责任置于个人的舒适之上。

更何况，这些承诺没有“保质期”：就算某人幻想破灭，离开了运动，但过了一段时间后在警方压力下供出了他们的“前”同伴，这种过错并不会因此减轻。

所以，我们将此视为一项原则：向敌人提供任何有关其他人的真实信息的行为都是不可接受的。既然违反这一规则会带来严重后果，那么这种违规行为本身就是一种重大过错。

剩下的唯一问题是，酷刑或其它因素是否可以作为一种“减轻罪责的情形”？

每况愈下的局面

诚然，我们能列举运动成员在镇压面前向当局提供重要情报的先例。

2010年的事件尤为鲜明。当时，无论是在俄罗斯（金奇市市府遇袭事件后）还是在白俄罗斯（一系列直接行动袭击事件发生后），无政府主义运动几乎同时遭遇镇压。据我们所知，当时酷刑仅在极少数个案中使用，其残酷程度也低于我们自2017年以来所见的案例。然而，在这两个国家中，都有人最终与警方合作。在所有已确认的案例中，社

群都对告密者进行了谴责和驱逐。

也就是说，无政府主义的“集体意识”所遵循的原则是：在面对威胁、恐惧和心理操纵时，供出同伴的行为没有任何正当理由。这种立场是难以辩驳的。

无论你正受到威胁，还是审讯者正在扮演“好警察”的角色，站在你面前的就是敌人。我们有义务不向敌人提供任何关于我们的同伴的信息。

即使是一个年轻的、刚加入运动不久的新成员受到警方施压，人们也期望此人在加入激进社群之初就已经具备了一定的预设道德准则，而其中“绝不出卖朋友”的原则应当是首要的。

虽令人遗憾，但近年经验告诉我们必须重申这一点。十年前，无政府主义圈子里根本不存在对“告发同志”持宽容态度的问题。过去并非更好，只是更容易。

总结来说：在言语和心理胁迫下向国家提供情报显然不可接受。但如果是肉体酷刑呢？

革命者的经验

翻阅过去革命组织的文献，我们很难找到针对酷刑下口供的具体态度。《人民意志》执行委员会的章程只是简要规定，要将组织的所有秘密深藏不露。

卡洛斯·马里盖拉的《城市游击队迷你手册》也仅用简短一行未作细述地指出：“那些主动向警察告发、指控、提供情报、和指认同伴的人，一旦被城市游击队抓获，必须予以处决。”

有意思的是，在描绘马里盖拉及其同伴斗争的电影《九月四日》中，

角色们毫不怀疑他们被捕的战友会在酷刑下供出情报。然而，他们最终还是将他解救了出来。电影毕竟是电影，现实情况如何，作者不得而知。

爱尔兰共和军的《绿皮书》花费了大量篇幅进行心理准备，以应对逮捕、审讯和殴打，帮助游击队员保持沉默。然而，文本并没有直接对酷刑下的供词进行道德评价。而且，《绿皮书》中提到的酷刑仅限于殴打和烟头灼烧。电缆连接生殖器和长时间电击枪电击的手段或许超出了1970年代北爱尔兰的现实范畴 —— 当代俄罗斯和白俄罗斯特勤警察的酷刑手段则更为残暴。

因此，在任何情况下都不作证的原则，与其说是明文规定，不如说是革命运动的一条不成文的规则，是一种被默认的不言而喻的共识。

二战期间的苏联，游击队员和地下战士无论遭受盖世太保何种酷刑，出卖战友都被视为不可接受的行为。例如，“青年近卫军”（苏联在德占城市克拉斯诺顿的地抵抗组织）的政委维克多·特雷蒂亚科维奇，至今仍是一个有争议的人物，因为有人怀疑他在被处决前未能经受住酷刑，向纳粹供出了名字和地址，尽管这一说法被许多人反驳。

有人认为，落在“专业审讯者”手中，没有人能经受住酷刑。这种观点并非毫无根据，但它不是事实。有许多文件记载了前辈们忍受可怕酷刑仍坚守信念的例子。下面就是一个。

左翼社会革命党成员鲍里斯·顿斯科伊于**1918**年在基辅刺杀了德国占领军司令赫尔曼·冯·艾希霍恩。鲍里斯在行动现场被捕。他的战友伊琳娜·卡霍夫斯卡娅在回忆录中写道：“他被带到监狱后，立即被绑在床上，遭受酷刑，要求他供出同伴。他们折磨了他三天，轮番上阵：他们烧、刺、割，将大头针和铁钉捅进指甲缝，拔掉了他所有的脚趾甲……” 顿斯科伊只说了他自己的姓名、籍贯、党派归属和行动动机。 关于战友的信息，他一字未提。他的“口供”实际上变成了一份政治声明。

这样的例子绝非孤例。

[image]

如何抵抗酷刑？

每一个经历过酷刑，甚至只是在警察局遭受殴打的人，都深知那是多么可怕、痛苦和羞辱。也深知要做到不屈服、不给施刑者他们想要的东西，有多么困难。

施虐者的目的在于摧毁你的精神意志。于是应对的关键在于保持清醒意识，根据情境灵活应对——或佯装恐惧，或夸大肉体痛苦，或以其他方式迷惑施虐者。

抵抗酷刑的方法是我们几乎从不公开谈论的话题。公开可说的仅有：当痛苦难以承受时，编造一个不涉及真实人物和信息的虚假事件版本或许能起作用 —— 将这个故事“固化”在脑中，让自己相信其真实性，并在受刑时坚持讲述这个版本。

但当然，最好的办法还是保持沉默。

阿扎特·米夫塔霍夫（**Azat Miftakhov**）向我们展示了另一种有效的行动方式。当条子开始对他施加酷刑时，他自己割伤了手腕（非致命的横切），迫使施刑者不得不停止施行并呼叫医生。他们害怕他死掉就得不到口供了。

[image] 阿扎特·米夫塔霍夫受审的新闻图像

面对出卖，纠问式应对方式错在哪里？

我们坚持认为，向镇压机关出卖同伴和泄露情报永远不可能是“正常的”或“可以接受的”。酷刑的情况也不例外。运动和我们每个人个人的原则只能是：宁可遭受酷刑、坐牢甚至死亡，也不能背叛同伴，不能向敌人提供重要信息。

当你听到有人说“酷刑下的证词无需负责”时，你会对这个人失去所有信任。你会意识到，只要轻轻一巴掌，就足以让他们全盘托出。将此类态度奉为圭臬的运动，永远无法吸引并培养坚韧的成员。没有坚韧的人，就不会有激进的变革。

但是，“任何提供信息的人都是叛徒” 这一立场又错在哪里呢？是的，抵抗酷刑是现实可行的。但很明显，即使是那些愿意抵抗的人，也并非所有人都能成功。任何没有亲身经历过残酷酷刑的人，都无法保证自己在那种情况下的行为。

那些曾经一度抵抗了施刑者、但在真正残酷的肉体压力下最终还是屈服供述者，很难再继续做我们的同志，成为无政府主义运动的参与者（尽管，当然，每个案例都必须单独考虑）。但是，将这样一个人轻易地定性为叛徒，并认为他们理应遭受报复，这公平吗？可能不公平。

[image]

这一论点不应与容忍供出同伴的行为相混淆。

供出同伴永远都是一个严重的错误。

尽一切可能，甚至付出更多代价，以保持清白，是每个人的责任。

否则我们何以相依为命？

杜波夫斯基案

白俄罗斯无政府主义游击队成员德米特里·杜波夫斯基(Dmitry Nikolaevich Dubovsky) 的行为在运动内部引起了巨大的争议。此案虽不涉及酷刑，但既然我们在讨论招供和屈服于审讯者的问题，就不可能忽略这个最近的例子。

否认杜波夫斯基在录像调查程序中言辞过多实属愚蠢 —— 他详细描述了成员站位及汽油瓶交接过程。当局和公众本无需知晓这些细节。但他的解释 —— 他与战友事先约定若遭拘捕则不否认行动，以此作为政治宣言——完全值得采信。若非如此，该组织的其他成员早就站出来否认了。至少在其他成员对情况发表评论之前，谁又能更清楚呢？

也许杜波夫斯基是出于困惑和错误判断而未能完全履行约定。有些人急于给他贴上“告密者和叛徒”的标签 —— 这对一位革命者来说是最严重的指控。此举恰是上述“纠问式”思维的典型体现。欲如此污名化他人，需有充分依据，而本案中我们并不具备充分依据。

[image]

总的来说，此案凸显了一个棘手问题：法庭如何成为政治讲坛。

这在革命史上实属经典实践。

审讯与庭审中的言论可成为强大的革命宣传手段，但前提是：必须公开表明立场，甚至可能需要部分行动配合。

核心问题在于：被囚同志的行为究竟是为在狱中开展宣传呢，还是为保全自身而为？

[image]

评判标准可以是：供词是否导致了新的逮捕？是否暴露了运动的内部运作？是否恶化了其他囚犯的命运，同时减轻了供词者的处境？这些声明是否有助于宣传行动背后的理念？

此外，在集体被捕的情况下，其他被捕同志的同意至关重要 —— 在此类关键事件上独断专行是绝不可取的。

根据所提出的标准，没有真正的理由指控德米特里·杜波夫斯基犯有叛国和告密罪。

[image] 2020年10月28日至29日晚，无政府主义活动家德米特里·杜波夫斯基在越过白俄罗斯边境时被抓，并被指控犯有“纵火”和“恐怖主义”。被判服刑20年。

再说几句

酷刑问题还有另外两个重要方面。

其一是：酷刑的现实，使我们通过个人的感官体验，而非抽象的言辞世界，认识到国家及其代表是我们的真正敌人，他们残酷而卑鄙。我们必须严肃而有力地与他们战斗。

其二是：运动必须保护自身免受叛徒的侵害。

如果我们谈论的是一场严肃的斗争，那些主动向镇压当局提供大量情报、并在后续调查中予以证实的出卖者，必须承受报应 —— 正如革命尚未沦为虚饰的年代里对类似事件的处理那样。

迄今当代无政府主义者尚未严肃探讨此问题。将报复机制纳入无政府主义运动体系，是我们亟待完成的重要任务，尽管听来令人不寒而栗。

结论

现代趋势 —— 全面的自我中心主义、沉迷于自身的“创伤”及其“治愈”——不利于抵抗国家镇压。如果认为只有个人舒适和幸福是首要任务，那么距离将它们置于信念、道德原则和同伴的人身安危之上，就只有两步之遥了。

当代文化提倡为软弱辩护。仿佛在困难的情况下不展现勇气和其他非

凡品质，而是崩溃放弃，是一种’神圣的人权‘。仁慈的态度与对能力边界的理解固然必要，但为软弱辩护是恶性的，且明显具有破坏性。

诚然，要求在酷刑下拒绝作证需要非凡的坚韧，但这种要求植根于我们的文化，自童年起便伴随我们成长。

此刻，软弱的权利不再适用，展现内在力量的义务才真正具有意义。

菲尔·库兹涅佐夫及同志们

无政府主义斗士

[image]
[image]

“我的”朋友还是“我们”的朋友？：如何执行担保措施

[image] 关键词	关系 准备工作 团队 安全文化 担保
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病
[image] 创建时间	2025年1月9日
[image] **Description**	关系结构革命；反渗透和协作

在激进派圈子里，“人脉”不是“资产”，而是严肃的安全问题。面对渗透破坏无孔不入的威胁，介绍新人加入队伍需要一套严格的标准和流程，以将未来发生事故的几率降至最低。本集内容将在具体策略方面给出一些建议。

- Table of Contents

  可靠性
  综上所述，就可靠性而言，最强力的担保对象应符合以下条件：
  胜任力
  综上所述，就身心胜任力而言，最强力的担保对象应符合以下条件：
  声誉
  宽恕和断交

[image]

“做担保”，即中文常言之“替人背书”。

对于激进社群中不同战友来说，“背书”的具体意义可能各不相同。对一些人而言，给某人做担保，意味着认为被担保人是值得信赖的，并且有足够的能力参与行动；而对另一些人而言，背书则意味着背书人拥有关于被背书人在忠诚度与能力方面的扎实证据，并愿意用自己的声誉为这些证据作保。

为了在“是否该为某人背书”这一问题上达成共识，我们必须明确“背书”的界定。

建议将背书分解为三个维度，有助于展开讨论：A, 可靠性、B, 胜任力、以及 **C,** 背书人的声誉。

- 可靠性：指被担保人是否已经或将会（无论有意还是无意）协助执法部门。这包括证明：被担保人目前及过去从未担任过执法人员或渗透者；从未担任过且目前也不是秘密线人；具有安全文化素养，不吹牛、不炫耀，不会有意或无意向没有参与行动的人泄露信息；且原则性强、意志力强，未来也很大程度上不会配合任何警方调查，即使面临牢狱之灾。

- 胜任力：指被担保人的自身能力和实力，即在身心素质上是否足以完成拟定的行动 —— 包括不会在行动开始前临阵脱逃、不会在行动过程中惊恐发作，也不至于陷入身体机能丧失的状态。

- 背书人的声誉：指万一给出“错误背书”的后果。根据违规的严重程度和行动本身的风险性，担保人的声誉后果的范围可能很广：从未来不再被严肃对待，到再也没有人愿意与该担保人或被担保人共同行动。甚至可能因欺骗或严重失职而遭到报复。

下文将详细说明评估被担保人可靠性与胜任力的证据强度，并简要讨论担保人的声誉以及错误担保的后果。

可靠性

如果想让别人相信你所担保的人值得信赖，那么你需要先仔细考虑一下能拿出什么证据来支持你的说法，这很必要。随着行动风险升高、被捕后果的加重，在激进社群中给他人做担保，所需要的可靠性证据强度也应随之提高。

以下是关于被担保人可靠性证据的一些建议，按强度由弱到强排列：

1. 通过与此人交谈，你是否觉得他们的态度和信念是真诚的？

空谈是廉价的，但人们往往能从直觉上判断一个人是否真的在意他们所谈论的话题。

读克鲁泡特金、施蒂纳、隐形委员会、或者《火焰万岁》这类书，并不是“普通人”的爱好，尤其是警察条子们通常都没有这般雅兴。所以……

[image]

从言谈上看，此人是否对某些事物充满激情？

此人是否有基本的安全通讯意识（对安全文化规则的信仰和素养）？

此人提议的活动（包括激进的违法活动）是否与你们之间的关系深度相符？

此人是否会不分场合地公开谈论自己或他人参与过的高度敏感活动？

1. 此人是否曾在没有他人促动的情况下，独立开展过行动？

虽然“知情权最小化原则”理想状态下应拒绝对他人从事的高度敏感活动的了解，但有时信息是可以串联起来的。当一个人不需要你或他人参与就能主动采取行动时，这表明其反抗情感是真诚的；尤其是，如果该项行动的确对统治系统具有破坏性，那么此人就不太可能是渗透者。

然而，尽管执法机构不鼓励犯罪，但是要知道：卧底和渗透者有时会被允许实施犯罪，甚至是他们自己发起并独立完成的。只要被渗透的目标组织被认为“值得”纳投名状，他们就会这样做。

所以仅此一点并不足以完全确定什么。尤其是要提醒，在知彼的同时，别忘了知己。

1. 此人是否曾与你共同参与行动，并对执法部门以外的人守口如瓶？

一个寻常错误是对行动及其结果感到兴奋（尤其是当行动上了头条新闻时），就忍不住向他人吹嘘。

[image]

一份强有力的担保必需意味着确定被担保人 始终能管住嘴 ，特别是在有大好机会炫耀的情况下，此人应有足够的意志力坚定地保持沉默。

1. 你是否曾与此人共同行动，并且，如果此人是内鬼，事情早就败露了？

被担保人曾经参与该行动，并知道都有谁参与其中 —— 这些信息足以让大家面临重刑。但至今无人被起诉。

这是一个非常强有力的指标，表明此人目前不是（至少目前还不是）渗透者或秘密线人 —— 除非他们正在“钓大鱼”（例如为了勾勒完整的组织网络图，或者希望抓获更重的罪名。这要具体分析）。

[image]

如果一个被担保人在长期、多种背景下参与了高风险行动（如涉及重罪的行动），且没有向该行动小组以外的其他任何人泄露过任何相关信息，那么这就是可靠性的体现。

1. 此人是否即使在面临严厉惩罚时，依然守口如瓶？

我们从许多案例中吸取了教训：许多死硬派无政府主义者宣称自己绝不告密，而且在顺风顺水时确实如此。然而，一旦他们被捕并面临长达数年的监禁，情况就会发生变化。 [image]如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04

[image]

对战友可靠性的终极考验，是得知他们曾有过通过配合检方达成诉辩交易来获得减刑的机会，但他们拒绝合作，宁愿承受惩罚，哪怕这意味着更长的刑期。

即便到了这个程度，可靠性也不是百分之百保证的。一个曾经坐过牢、始终保持沉默的人，在面对超出其承受能力的崭新刑期时，也可能会动摇。在《终身监禁》一书中，巴尔的摩桑德敦的帮派成员在面临再次入狱的威胁时，最终选择了告密。在背书这件事上，从来没有万无一失。

综上所述，就可靠性而言，最强力的担保对象应符合以下条件：

1. 在交谈中展现出开展行动的真诚态度和信念。（政治信仰/政治认知/立场和精神）

1. 曾在没有你促动的情况下，独立或与其他小组开展过行动。（主动性）

1. 始终参与那些具备社交炫耀资本的行动，但从未对外吹嘘。（嘴严/靠谱）

1. 曾与他人共同参与足以导致长期监禁的严重行动，但从未出事。（成熟的能力）

1. 曾选择在监狱服刑，而非通过配合检方的诉辩交易来获得减刑。（德行/可信赖的同伴）

[image]

胜任力

根据我们的经验，担保人往往会几乎完全忽视被担保人完成行动的胜任力。虽然你喜欢并信任某人是一件好事，但如果对方并没有能力执行行动，那么让他们参与行动就是极不恰当的。

因此，在担保的考量中，胜任力与可靠性同样重要。我们认为，就担保而言，胜任力包含两个部分：心理素质与身体素质。

[image]

心理素质意味着该成员具备完成行动所需的心智能力，包括行动所需的特殊技能、知识、个人魅力或其他非体力属性；

但通常更重要的一点是，他们拥有强大的心理韧性，能在压力下保持专注而不惊慌失措。

如果一个人无法集中注意力、记不住自己的任务，或者虚报自己执行部分行动的能力，那么他就不应被视为具备从事该行动的胜任力。

身体素质意味着该成员在体力上能胜任行动。如果行动涉及奔跑，该成员必须具备奔跑能力（请注意，由于存在被警察追捕的风险，几乎所有行动都隐含了对奔跑能力的要求）。如果行动需要跳跃、骑行、攀爬、游泳、绳降、长距离徒步或背负重物，该成员必须能够胜任这些体力活。

与可靠性一样，最弱的胜任力担保仅凭对方“口头保证”有能力，而最强力的担保则源于对方确实拥有在行动中有效完成此类任务的既往记录。

以下是关于心理素质证据的一些建议，按强度由弱到强排列：

- 被担保人是否声称自己知道行动中所需的所有操作？

空谈是廉价的，但至少担保人应与被担保人进行充分沟通，确保对方理解行动要求，且被担保人至少在口头确认过自认为能够胜任。

- 在交谈中，被担保人是否展现出关于如何完成行动任务的专业知识？

讨论很重要。通过讨论通常可以了解一个人的心理储备。例如，如果行动涉及爬树，而对方连如何打“8字结”都说不清楚，那么他们很可能不具备所需的胜任力。

- 在交谈中，被担保人是否证明了自己能记住行动计划的分工，并能够思考 周密的行动计划 中所有细节？

如果被担保人丢三落四、在谈话中无法集中注意力，或者看不出任务中显而易见的逻辑 —— 比如在使用可能留下[image]指纹 的器材时想不到要带哪种 [image]手套 —— 那么他们就不太可能在行动中保持专注，可能会连累其他人。

- 在交谈中，被担保人是否展现出能通盘考虑整个行动计划、洞察优缺点并提出应对方案的能力？

能够推敲整体计划、寻找漏洞并尽力弥补，说明此人理解行动的本质，能在思考时留住关键信息，并可能在出问题时做出必要的调整。

一个无法理清计划的人，在必要时也不太可能做出有效的临场变通。

- 被担保人是否在非行动背景下展示过行动所需的技能？

回到“8字结”的例子，如果一个人能在非行动背景下，无需他人帮助

就能快速可靠地打好结，这是该人“言行一致”的良好指标。但这并不代表在压力巨大、肾上腺素飙升时，他们依然能打好这个结。

- 被担保人是否在实际行动背景下展示过相关技能？

利用无线电通讯规避警察是一种技能。如果担保人根据以往经验，亲眼见过被担保人具备这种规避能力，那么这是一个强有力的指标。

[image]

在真实行动的巨大压力下完成任务，与在低风险场景下展示知识，是完全两回事。

- 被担保人是否在多次高风险行动中 证明 了自己具备相关技能，并能在压力下运用这些技能？

被担保人一次又一次地在重压下完成了任务。他极少犯错，且在犯错时能够设法弥补。这可以是很高的可靠性指标。

- 被担保人是否在多次高风险行动中证明了自己能保持冷静专注，即使出事也能临场想出解决方案？

有效处理高风险行动中的意外，是对心理素质的最高考验。这要求参与者能调动背景知识、方案细节、敌方战术信息，并保持足够的冷静，以将这些知识转化为新计划。

身体素质的证据亦然：最弱的证据来自谈话或日常观察，最强的证据则来自高风险背景下的直接共事。当面临逮捕或受伤的迫切危险、肾上腺素飙升时，人的双腿可能会发软，会突然想要排泄，甚至可能昏厥、哮喘发作、甚至出现心脏问题。最好的证据，莫过于亲眼看见过被担保人在极端高压场景下依然能掌控自己的身体状况。

综上所述，就身心胜任力而言，最强力的担保对象应符合以下条件：

1. 声称自己在身心两方面都能胜任行动。

1. 在交谈中展现出完成行动所需的操作常识。

1. 证明自己能规划并周密思考自己负责的部分。

1. 能够通盘推敲整体计划，并分析其优缺点。

1. 在非行动背景下展示过相关技能和体力。

1. 在实际行动背景下展示过相关技能和体力。

1. 在多次高风险行动中证明了即使在压力和意外面前，依然具备所需的技能和体能。

[image]

声誉

对于低风险的小型行动，一次糟糕的背书通常不算大事。我们可以谈谈哪里出了问题，并尝试达成共识。然而，如果为那些告密者、管不住嘴的吹嘘者，或者因身心问题完全无法执行行动的人做担保，那可就是大问题了。

虽然告密显然是担保失败最惨痛的结果，但由于多嘴或恐慌而成为行动小组的累赘，同样极难处理。

任何给出担保的人都应明白，你的声誉取决于你作出的担保，被担保人的行为会直接反映担保人的信用。明确这一点的目的并不是让人在背书时变得神经质或斤斤计较，也不是为了建立某种惩罚性的社会等级，而是为了让人们严肃对待自己在做担保时作出的承诺。

宽恕和断交

人们在行动、言论和背书中都会犯错。在大多数情况下，讨论并宽恕一些次要问题是值得的。即使经验丰富的激进派活动家也可能恐慌或失误。通常出现的胜任力问题往往是可以被原谅的，因为这通常不代表恶意，仅仅意味着知识不足。

但可靠性方面的问题通常要严重得多。有一个能力不足的战友并不代表心存歹念；但如果有一个压根不靠谱的战友，即使是无心之失（例如不小心漏嘴说出了某人的真实姓名且掩盖得很拙劣），危害是极大的。更不用说告密或者向行动组之外的人谈论敏感行动了，那绝不是意外，而是选择——这种选择几乎不值得任何宽恕。

[image]

请记住，如果你为不可靠的人背书并继续与其往来，你自己也会被视为不可靠。

如果不与那些蓄意伤害我们的人断绝关系，那么我们所有人都会处于危险之中。

如果我们不与他人共同承担风险，那我们也就失去了成就伟业的机会。

□

[image]
[image]

S07 审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

[image] 关键词	个人 亲密团队 反渗透 团队 基准线 审讯心理学 心理安全 战友 线人 诱供 逮捕
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；审讯心理学
[image] 创建时间	2025年3月1日
[image] **Description**	心理安全；反渗透和协作

[image]

返回 - 镇压手段：审讯心理学

本系列我们将聊一些“不愉快”的话题 —— 被捕、受审、酷刑，也包括狱中的生存技巧；以及一个尤其艰难的议题：如果您的亲密同伴被捕并遭受酷刑，而后被释放，他/她说自己没有出卖任何人，您还信任他/她吗？……

某种程度上，现实比电影更加残酷。

本站绝大部份内容的主旨均在于避免被捕，毫无疑问，“不被抓到”是革命者的首要任务。但我们也同时必须为最坏情况最准备，因为只有这样，只有尽可能减少后顾之忧，才能让我们的行动更加自由和安心。

为最坏情况最好准备，才更有力量迎接最好的结果。

被捕和入狱都不是“结束”，相反，它们是整个抵抗斗争的一个阶段——尽管是最艰难最糟糕的阶段，但我们的确有办法通过学习前人经验和各方面细致的准备工作而让这一阶段更平安地过渡。

不要被摧毁。不要被操纵。要全须全尾地取得胜利。

[image]

S07系列中有一大部分内容应该可算作反渗透主题，因为审讯过程中采取的心理操纵和胁迫的原理与渗透者的招式基本一致（也因此我们将其同步于反渗透知识库）。将审讯场景单独提出来是应前线学习者的要求，并且我们也意识到相关内容的确值得更多的补充。

[image]
当前本系列的体量还很小，未来期待更多补充。尤其追求两方面的资源：警用审讯培训资料，和亲身经历者的一手经验。不分语种，随时欢迎翻译合作！
[image]

列表

[image] 您是如何被困住的：审讯心理学 S07E01

[image] 巧妙的威胁：审讯心理学 S07E02

[image] 无政府主义者生存指南: 了解盖世太保猪式审讯心理游戏 -审讯心理学 S07E03

[image] 如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04

[image] 在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学S07E05

[image]
[image]

您是如何被困住的：审讯心理学 S07E01

[image] 关键词	反渗透 审讯心理学
[image] 关联	[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛 🙈渗透者 ；□告密者（线人）
[image] 创建时间	2025年3月2日
[image] **Description**	心理安全；反渗透和协作

关于如何过招、以及您应该在什么情况下怀疑对方的身份和目的。

- Table of Contents

  1、让对方感觉到被孤立是取胜的法宝
  2、故意在对手组织内部制造矛盾
  3、从细微之处突破对方的心理防线
  4、解读行为举止

[image]

渗透进入目标组织内部的间谍经常采取主动出击的方法，以尽快掌握主动权。

由于环境不同，他们采取的具体措施各不相同，但是目的性都很明确。这是与普通人的一个重要区别，普通人犯糊涂和性情偏激并不奇怪，但是不会有如此强的目的性。

并且，很多时候线人不会与他们的目标正面接触，而是采取迂回战

术，从各个侧面包抄、包括利用无知的旁人做手套；目的是使目标人处于一种孤立无援的状态，再发起直接的进攻，便有更大的胜算。

这种手段极为常见，而且能达到出奇制胜的效果。

即便是强大的人，一旦被孤立起来，就会变成一只困兽，不再具有反攻能力。

[image]

反过来说，如果您发现您的组织内部出现有步骤有目的的拉帮结派分化孤立的操作，当提高警惕，并尽可能迅速找到背后的操纵者 —— 渗透者经常会想办法让事件看起来与自己无关，他们会利用一堆无辜的（也是无脑之人）为自己做掩护。

以下将分析这种手段如何操作，尤其是如何防御。

[image]

在此之前需要提示一点点概念问题。

人们使用过很多名词来形容从事间谍活动的特定人物，比如线人、线民、变节者、墙头草、硕鼠 …… 等等，但必须说，理论上渗透者和线人不完全相同。

[image]

返回 - 镇压手段 - 在这里看到渗透和告密的区别：渗透者 ；告密者（线人）

渗透者指的是您的对手雇佣的人。也因此，渗透者被高度控制，是不容易被转化的。而线人、告密者等其他概念均包括没有专门为您的对手服务的人，他们可能因各种原因站到敌对方一边去了 —— 包括组织内部的争议演变为变节、自身薄弱环节被对手拿捏并因此被操纵，等等都有可能。这类人还没有被您的对手完全控制，是相比下容易被转化的。

对于后者，圈子江湖的山头之争中很常见。竞争对手向警察告密，为的不是帮助警察取证，而是借助警察的力量打击自己的对手。

也因此，有些时候警方间谍会故意在“山头”之间挑起纷争，以促进告密者的出现。

所以说， 权力等级是一种致命的安全威胁。

1、让对方感觉到被孤立是取胜的法宝

这是每一个接受过相关培训的间谍都懂得的道理。

就如任何一种攻击之所以能成功的关键一样，这种操作首先要做的就是对其目标进行全面的心理分析，并透彻理解，从而准确抓住目标人的心理弱点。

[image]

故而，再一次强调，您平时暴露自己的内心越多、在网上说的越多，您的弱点就会越明显。

因为您永远不会知道有谁正在观察和揣摩您，以及他们都是什么目的。

这种心理攻击手段也经常出现在审讯中。

如果被审讯者坚持零口供，审讯人就会采取瓦解士气的心理攻击策略，从侧面进攻，往往会起到意想不到的效果。

让对方感觉孤立无援是实施打击的第一步；准确掌握对方的心理弱

点，是实施孤立战术的基础。

中国读者应该对心理战非常熟悉了，中国古代的兵书中就强调过这点："谋事不以力，而以攻心为上"。也就是说，心理战术的效果经常会强过武力，与武力协调使用将事半功倍。

同样道理，间谍对目标人和群体展开的进攻大多运用这种方式。一个人只要从心理上被打败了，纵然是拥有庞大的兵力，也是丝毫没有战斗力的。

于是，反制的方法也来自同一思路。

斯诺登在第一次揭秘后就立刻面临了强大的威胁；美国下达了全球通缉令，许多国家都碍于地缘政治利益而拒绝给予斯诺登政治庇护。

但是斯诺登继续曝光接下来的一系列文件，而不是就此隐藏起来。表面上看起来这似乎是"绝路"？

事实上是一种反制策略。

因为在第一份文件曝光后他已经成为了联邦政府和间谍机构的敌人，无论如何都不会改变这点；于是，在这种情况下有可能保护自己的方法就是加深这种敌对关系，而不是"回头"。

如果斯诺登在第一次曝光后便停止，听从国安局的"公开劝诫"、不再继续所谓的"叛国之举"的话，那么他的安全将受到极大的威胁。

[image]

他会因此迅速失去最强大的支持者—— 这就是为什么国安局从不强调惩罚，而是公开"善意/原谅/鼓励"，以诱使目标心理动摇，从而迅速被孤立，之后只能是快速被击破。

美国当局虽然发起了全球通缉，但并没有真正真正部署具体行动；美

国间谍组织和情报共享网络是全球一流的，如果他们想做，绝对能做得到。

但是相反，国安局并没有立刻实施追捕和暗杀，而是频频向斯诺登“示好”，他们不止一次公开宣称，只要停止揭露文件他们将撤销通缉令，并恢复护照的合法性；与此同时，国安局还对任何同情斯诺登的组织和国家施加压力，令他们放弃，以孤立斯诺登。

比如从一开始便允诺为斯诺登提供庇护的冰岛和厄瓜多尔政府，被美国利用外交和贸易等手段施加压力，最终导致两国都转变了对斯诺登的态度。

因为他们知道，只要斯诺登答应不再继续曝光，他就会迅速失去那些一直在帮助他和组织和政府的支持；将斯诺登孤立起来，国安局就能随意处置他了。

在这场较量中，斯诺登作为表面上被动的一方，实际上从一开始就掌握了主动地位。

因为他懂得国安局监视的常用手段。只要他停止曝光，很快就会淡出人们的视野，这样他就会面临更大的危险。

相反，只要他能做到持续曝光，在全球人的瞩目下国安局就不敢对他下手。因为一旦国安局动手，就相当于主动承认了斯诺登对他们指责。

□

在街头对抗中“反制”策略也是至关重要的一种 - 将您的对手置于决策困境：https://iyouport.substack.com/p/f2a?utm_source=publication-search

反制，即 使用同样的策略反守为攻，将针对您的人孤立起来。

国安局间谍全球的内幕曝光后虽然没能终止各种被揭露的监视手段，但是，绝对在地缘政治角度上产生了强大的影响，斯诺登是真赢家。

[image]

2、故意在对手组织内部制造矛盾

在孤立对手的同时，间谍往往都会使用各种各样的其他手段，甚至包括约炮，都可以是手段的一种；具体介绍参见 [image]什么是“秘密行动”？政府间谍会怎么折腾你... 。

二战期间著名的女间谍弗吉尼亚·霍尔年轻的时候在一次打猎的过程中伤到了左脚，导致膝盖以下被截肢，但这并没有影响她成为一名出色的间谍。

军情六处招募她为外线间谍，她装上假肢后就被派往了法国里昂。

在战争期间，为了安全起见，大多数间谍在同一个地方停留时间不会超过三个月，但弗吉尼亚·霍尔由于出色的间谍技能，在里昂一次停留就是十五个月。

随后她又被派往伦敦，为中央情报局设立的战略服务办公室提供情报。

弗吉尼亚·霍尔受到全球两大情报机构的青睐，主要因为对其他间谍来说艰难的任务她每一次都能出色完成。

在纳粹统治区工作的时候，当时她的任务除了搜集关于纳粹的情报之外（被动任务），还有一个主动任务，就是从内部瓦解对手，为英美联军实施最后的总攻做好准备。

霍尔接受过专业训练，她知道要成功完成这项任务就必须实施巧妙的心理战术。但是当时的处境导致她根本无法主动出面。

因为盖世太保正在四处缉拿她，并且他们还知道她是“一个跛脚女人”。这对于霍尔来说非常不利。另一方面，在当时的纳粹军中散布不利信息也几乎不可能。

[image]

霍尔在后来的回忆中写道：要想打击敌军，令其失去战斗力，关键在于瓦解其军心，最好的办法就是在敌人内部制造一种矛盾，从而让敌人的军队完全被孤立起来。

她的方法说起来并不复杂。因为在当时，不仅是德国，所有卷入战争的国家的人民都对战争充满了恐惧和厌恶。战争导致他们流离失所甚至家破人亡。

这对弗吉尼亚·霍尔来说是一个绝佳的切入点。她利用有限时间频频潜入当地驻军的城市或村庄，向当地人讲述战争的危害。借助人们的怨气，她迅速获得了热烈的支持。

由于是驻军地区，纳粹军经常要与当地人接触，于是人们在不知不觉中就把这份怨气传递给了那些纳粹士兵。

最初纳粹士兵只是将其视为一种简单的抱怨，并没有真的放在心上，但是听得越来越多之后，这些士兵在回到军营谈起自己的家人时，也开始为家人担忧。

借助情感传递将这份内部分化的情绪迅速传播开了。没多久，一股厌恶的情绪开始在军中蔓延。很多士兵感觉到了战争的冷酷无情，于是纷纷逃离军营，参加了当地的反战组织。

如此，整个军队逐渐成为一支被大多数人民所抛弃的军队。尽管控制权依旧被希特勒牢牢掌握，但实际上他已经被孤立起来了。

因为孤立不仅仅是来自人民大众的反对，还来自希特勒十分信赖的军队内部。

□

延伸 - 战术原理：https://iyouport.substack.com/p/62?utm_source=publication-search

在纳粹投降之前，纳粹军队就几乎失去了战斗力。整个军队的士气已经被瓦解，不论战斗力有多强大都注定会失败。

弗吉尼亚·霍尔的侧面心理攻势起到了很大的作用。

[image]

这里的"敌""我"并没有确定的善恶之分，默认心理战的实施者为"我"、其目标为"敌"。无论是地缘政治斗争还是国内对反对派群体的渗透，都是同样的道理。

从内部瓦解对手组织的士气这一心理战术是各国间谍的必修课。

如前所述，审讯中也一样。审讯一般都是分开单独进行的，审讯者做的就是采取心理攻势，努力孤立各方，让被审讯者认为自己的伙伴已经叛变。

[image]

3、从细微之处突破对方的心理防线

如前所述，孤立对手是常用的办法。但是在有些时候，做到这点不会太容易。于是间谍往往会尝试突破对方的心理防线。

从细微之处入手寻找切入点。

还以斯诺登的经历为例。国安局间谍就是利用这种方法挑起斯诺登和

阿桑奇之间的矛盾，试图将斯诺登完全孤立起来。尽管没有真正成功，但却在一定程度上离间了斯诺登和维基解密。

这种心理攻势也是间谍培训中的一个重点：哪怕是做事十分谨慎的人，其身上都存在某种不可改变的个性或性格缺陷。即便受过专业培训，有着超强的心理素质，知道该如何更好地保护自己不被发现，但其内心深处的弱点往往很难克服。

这是人性使然，没有十全十美的人。

但是要发现这一弱点并不容易。中情局的反间谍专家曾经说过："反攻应该从人性角度入手，以便找到心理突破口"。

从国安局对斯诺登的手段中可以看出，间谍们将斯诺登留在美国的家人当成了切入点；与此同时他们还了解斯诺登是一个重感情的人，必定会对其家人十分看重。

于是国安局的间谍便由此展开了心理攻势：一方面他们通过媒体放大"劝说"性的信息，并谎称只要斯诺登放弃曝光他们就会撤销全球通缉令；而另一方面，他们又派出特工突击斯诺登家人的心理防线。

他们采取的是迂回战术：并没有直接用斯诺登的安全问题做武器，而是转向了阿桑奇。

对于斯诺登的父亲而言，他已经从报纸上知道了自己儿子的处境，也知道阿桑奇是唯一直接帮助斯诺登的人。而且他也明白，家中的所有通信都被监听了。所以家人对斯诺登情况的了解其实并不多。

于是国安局就利用这点，在斯诺登家人面前诋毁阿桑奇，谎称阿桑奇"借助斯诺登到处敛钱"。

事实上这一切完全没有任何证据。国安局利用的是曼宁的例子，做了一口黑锅给阿桑奇。

因为当时曼宁曝光文件后奥巴马政府立刻起诉了曼宁，虽然所有被起诉的罪名并没有被法官一一批准，但最终还是被判刑了。这些资料在各大媒体上公开，所有人都知道。

但联邦调查局很快发现，曼宁的支持者非常多，人们不仅没有被当局的起诉和污蔑所动摇，并且组织起来为曼宁集资了125万美元。

125万美元的确是事实，但国安局陈述的内容完全是虚构的，他们将这笔钱栽赃在了阿桑奇身上，并讲给斯诺登的父亲，谎称“阿桑奇借曼宁收敛支持者的钱财”。这就是人格暗杀的一部分。

□

延伸：

在谎言的压力下，斯诺登的父亲果然受到了影响，开始怀疑阿桑奇 —— 斯诺登唯一的最大的支持者，他也通过律师表达了同样的质疑。

国安局的目的十分明显，就是通过斯诺登的父亲离间斯诺登和阿桑奇之间的关系，在支持者之间制造猜忌，从而孤立斯诺登，以便进一步攻击他。

后来阿桑奇的助手及时赶到香港协助斯诺登避难，国安局的心理战才未能如愿。但是，这种心理战术非常值得警惕 —— 因为并非所有被瞄准的人都具备有效的反攻机会和能力。

尤其是，我们听说过中国当局也擅长胁迫异议人士的家人；于是您很有必要在防卫计划中将家人被突破的可能性纳入进去。

[image]

4、解读行为举止

探究到对方的心理弱点，然后针对性的发起攻势，从心理基本面上彻

底搞垮对方。

于是解读对方的行为举止被称为间谍能力的准绳。

[image]

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

举止比言语更容易暴露一个人的内心。观察并分析举止是间谍培训中的重点部分。

反过来看，间谍依靠谎言维生；虽然他们可以使用高明的谎言做到逻辑上滴水不漏，但也很难控制自己的行为举止，尤其是微表情。

从心理学角度上说，即便是再狡猾的间谍，在说谎或内心情绪波动时也无法逃脱微表情停留的极限，即1/25秒。这是人的生理因素决定的。

因此，细致观察对方的行为举止就能迅速了解对方的内心世界，从而根据对方的心理特点做出不同的应对策略。做到这点并不是太难，需要很多直觉方面的练习。

请注意，人们往往会因此认为，培训政府间谍的教程也适合反间谍人员学习，理论上的确如此；但是，要做到成功的反间谍，必需能在间谍基础知识的层面上高出一步，否则反而更容易被识破。

一个著名的案例。很多人都知道有着“21世纪间谍第一人”之称的罗伯特·汉森。当奥德里奇·艾姆斯被中情局和联邦调查局抓获后，两大情报组织发现，所有疑点都指向罗伯特·汉森。

他们派出了最优秀的间谍来调查此案，但是多年后一无所获。联邦调查局感觉难以置信，因为他们对汉森进行了多次测谎，但每一次都被他通过了。

直到继续对汉森进行长期监视才真的发现了蛛丝马迹。

本来汉森觉得只要能稳住一段时间就可以安全渡过难关；正因为多年来中情局和联邦调查局都没有发现任何事，他心里就有些得意了。也正因此放松了警惕。

在弗吉尼亚州维也纳小镇的公园里，他的确使用了基本反侦察技术对周边做了一些调查，确认安全后他将公文包放在了一个指定地点。

完成这一切很顺利。原本没什么问题，但是他发现两个可疑的人站在公园一角。当时他心里一慌，下意识地将外套衣领向上提了一下，然后放慢脚步离开。

结果就是这个拉衣领和突然放慢脚步的小动作将他出卖了。

那两个可疑人的确是联邦调查局特工，他们其实并没有发现公文包，由于跟踪汉森很久了，他们也在心理上放松了警惕；但是，直到看到汉森的两个小动作，立刻发现了异常。

随后便找到了那个公文包。

作为多年从事特工工作的人，汉森已经养成了伪装自然走路姿态的习惯，所以忽然的放慢脚步其实是他作为间谍的本能反应；然而这点恰恰被同样是间谍的联邦调查局特工捕获了。

所以，必须说，了解您的对手的知识和思考方式肯定是必要的，但如果您想要做到有效的反制，就必须比对手高出一筹。

[image]
[image]

巧妙的威胁：审讯心理学 S07E02

[image] 关键词	审讯心理学
[image] 关联	[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛 [image]信息最小化原则 ；分身 ；[image]对证据的偏见性解读
[image] 创建时间	2025年3月3日
[image] **Description**	心理安全；反渗透和协作

如果你不想对警察说的话都说在互联网上了，结果很可能比直接对警察说更糟糕。

- Table of Contents

1、巧用证据，逐步瓦解抵抗力
2、咆哮式审讯击毁心理防线
根据中情局的观点，咆哮式审讯有几点技巧：
3、语言攻势撕破心理伪装
A、音调方面的优势。
B、紧抓对方的疏漏。
4、制造绝望
A、不强行逼供。
B、要避免被对方看出己方实力。
5、疲劳战术。
6、多说不如少说。
7、诱导。

本文中分析的内容最适合审讯场景，如果您是活动家、记者、人权维护者、人权律师、边缘社区等任何挑战主流政治的人，您有必要了解这些；一旦被捕，您可以做到心里有数，并做出适当的合理的反应，

尽可能保全自己和队友。

[image]

返回 - 自卫措施：[image]镇压应对措施 ；[image]被捕支援

[image]

与前文不同，本文中即将讲述的方法更为主动，间谍采取此类方法是希望能达到立竿见影的效果。

即便没能立竿见影，也可以给对方制造强大的心理压力，以影响其之后的进攻。

[image]

恐吓也许是一种假象。但是被恐吓者往往会宁信其有，这是在借助信息不对称和心理映射，激发对方产生畏惧心理。

任何人都可以使用恐吓，使用者必需知道自己在对方面前的优势所在，强调这一优势以令对方害怕。

□

参见原理：https://iyouport.substack.com/p/34?utm_source=publication-search

不同的是，活动家对威胁战术的使用必需能有切实实施威胁的能力。

而在本文即将分析的威胁类型中，间谍并不需要真的实施威胁，只需要能让对方相信威胁的真实性。

以下部分将更多以审讯者的角度陈述，以帮助您了解您需要应付的人的思考方式。

1、巧用证据，逐步瓦解抵抗力

在审讯中所谓的“证据”经常被拿来施压，但什么时候使用证据、如何令证据发挥关键作用，是间谍课程的一个重点。

显然其要点也是心理战术。即攻心术。

有效的攻心术可以比酷刑的效果更高。

审讯者都明白，在长时间的心理战之后，被审讯者已经疲惫不堪，其思想会徘徊在招供和不招供之间。这个时候就是施加攻心术的最佳时机。

也就是说，在被审讯者思想波动幅度最大的时候，审讯者及时给对方足够的理由令其招供；令其感觉到没有其他选择。

这时候有力的证据就是一张王牌。

[image]

反过来看，不让您的对手拿到最致命的证据，是您能做得最好的反制策略。

1984时代，当局的证据基本都来自长期监视，不论是您的数字足迹还是您的在线和离线身份的关联，对您来说都是致命的。

所以，避免被攻心术击倒的最佳方案就是，从一开始就尽可能不要留下证据给对手。

[image]

返回 - 自卫措施：分身 ；[image]数字技术限制和最佳实践
；[image]信息最小化原则

[image]

如果使用了以上全部方法，但最终被亲友出卖而导致失去了反制机会，那么能保护您的方法就是撒谎 —— 如果您平时保护工作做得很好，应该就能有信心相信审讯者手中掌握的证据不多；于是即便有人出卖您，您也能有一个大致的危险性评估。

这一评估非常重要，将决定您在遭受攻心术时的抵抗力。

并且能决定您的撒谎计划的有效性 —— 目标是让对方的逻辑链断掉。

[image]

追求零口供的受审者往往通过保持沉默来抵抗，理论上可行，尽管不是所有情况下都能有很好的效果。某些情况下，如果审讯者只找到了您这么一个“线索”，您越是不说话，审讯者就越会觉得您隐瞒了很多。相反，如果审讯者手边有一大堆乱七八糟甚至完全矛盾的“线索”，您只要能坚持住拒绝说话，让他们意识到您难搞，他们就会转向其他更容易啃的骨头。

总之要随机应变！

熟知法律也很重要 —— 审讯者使用的都是套证据的方式，只要最终得不到有效的口供，就无法定罪。

只有证据才能让人认罪。在缺乏证据的时候，审讯者甚至会人为地创造“证据”，也就是栽赃。栽赃的信息往往不合逻辑，这种情况下你需要在律师到场之前不做任何评论。

不论是真实的证据还是栽赃， 审讯者都非常注重证据出示的时机，他们的目标是给被审讯者制造最强大的心理压力、给自己立威造势 。作为被审讯者您应该了解对手这一心理，如果您害怕就真的输了。

2、咆哮式审讯击毁心理防线

理论上咆哮不是暴力，但是它能制造一种压力氛围，尤其是它持续进行的情况下。

在咆哮的过程中，审讯者往往会以最激烈的语调讲述他们“获取的证据”，尤其是，穿插引用被审讯者的心理弱点 —— 比如父母、朋友、孩子。

内心缺乏安全感的人对咆哮式审讯的氛围会非常敏感，更容易中计而产生屈服心理。

[image]

这需要审讯者事先做出社交工程调研，以掌握被审讯者最脆弱的心理敏感部位。

反过来，被审讯者平时暴露自己的心理越多，这种情况下就会越危险。

人们经常觉得一些“不敏感的内容”可以在网上随便说，其实不然；所有这些信息综合在一起很容易暴露你的心理特征，令你的对手可以更准确地掌握攻心术的设置模型。

还是那句话，让对手对您的了解越少、了解得越不真实，您就越安全。

根据中情局的观点，咆哮式审讯有几点技巧：

A、“一怒到底”。

绝不可以浅尝；否则会陷入一种尴尬的境地。一旦罪犯的感情没能调

动起来，审讯者就输了。

需要持久、极致，在心理上占据高地。

B、“要果断”。

必需显得无比自信，即便审讯者自己并没有拿到切实证据，也必须表现得就像掌握全局一样，要看起来不容置疑。

这种氛围将迫使被审讯者内心展开自我审查；一旦自我审查的意识出现，被审讯者就会立刻虚弱，就离投降不远了。

C、“言之有物”。

咆哮不能仅仅是愤怒，如上所述，必需在咆哮中拿出切实证据。即便证据并不充分，在情绪压力的大环境下，被审讯者往往来不及仔细思考逻辑问题，从而屈服于不完整的证据。

或者说，证据不完整的时候，审讯者采取咆哮方式的可能性更大。

所以被审讯者需要能保持冷静。

[image]

3、语言攻势撕破心理伪装

语言攻势在很多情况下都可以使用，而不仅仅是对峙过程中。

这里指的语言攻势是以令对方折服为目的的，它具有两个特点：

A、音调方面的优势。

在交锋过程中音量会被试图放大，为的是能在心理上占据优势地位。

但是不能一味地放大，如果审讯者在拿出切实证据的那一刻依旧保持了极高的音量，反而会减弱证据的压力作用。

有效的语言攻势是音量合理起伏的，在持续高声的过程中忽然调低音量，将更容易吸引对方的注意力，令语言更加深入内心。

B、紧抓对方的疏漏。

俗话说百密一疏，疏漏可能是非常致命的。但是并非每一种疏漏都容易被发觉。当审讯者通过调查抓到了对方的疏漏时，就会在语言攻势中强化运用它，以瞄准被审讯者的心理弱点。

4、制造绝望

成功进攻他人内心的关键方法就是，让对方自觉已经断了后路。

绝望感会导致对方主动放弃挣扎，接下来的一切都随你处置了。

审讯者追求的就是这种调动您绝望的感受，要达成这一目的，必需要有切实依据，能真正触动对方的信息。

虽然这一信息很可能不值得深究，但只要它能制造强大的绝望感，几乎没有人会详细思考它为什么不合逻辑。

绝望是能杀死人的。

一旦萌生绝望感，对方就会迅速暴露心理弱点，审讯者将及时抓住这些线索，展开更加强大的攻势。

间谍在采取攻心战术时往往会遵循：

A、不强行逼供。

事实上外在的高压逼迫只会让对方产生更大的抵触心理。

相反，聪明的暗示可以让对方知难而退。

于是有经验的间谍会做得非常巧妙，一步步引导被审讯者走入绝望。

B、要避免被对方看出己方实力。

从心理学角度上，威胁的真实含义就是：实施者其实没有绝对的把握能战胜对方，他只是希望借助心理压力让对方主动投降。

换句话说，如果您是被审讯者，遇到上述心理攻势时切不可慌乱，因为让您慌乱正是对手的目的。

如上，是最常见的审讯心理战。此外其他方法还有：

5、疲劳战术。

这是针对心理素质很好的被审讯者所采取的方案。

这样的被审讯者绝不会主动交代，审讯者采取询问的方法是无效的，尤其是被反复提及的问题，更不会回复。

这种情况下审讯者会采取疲劳战术，直到对方倦怠，再准确抓住被审讯者的逻辑错误并强烈打击。

6、多说不如少说。

这也是一种心理技巧。目的是给对方一种神秘感，让对方摸不透审讯者究竟掌握了什么。这种神秘感有可能激发被审讯者的自我审查，从而进一步表现出心虚和不安。

7、诱导。

也就是利用语言学引诱对方说出对自己不利的信息，却不会感知到。

[image]

返回：👄语言是强大的武器 - 如何使用它？人性黑客：致命的诱导

返回：[image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”

[image]
[image]

无政府主义者生存指南: 了解盖世太保猪式审讯心理游戏 -审讯心理学 S07E03

[image] 关键词	亲密团队 审讯心理学 心理战 直接行动 社交工程 诱供
[image] 关联	[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛
[image] 创建时间	2025年3月4日
[image] **Description**	心理安全；反渗透和协作

闭嘴才有逃生的机会。

- Table of Contents

1、
2、
3、
4、
5、
6、
7、
8、
9、
10、
11、
12、
13、
14、
15、

16、
17、
18、
19、
20、
21、
22、
23、
24、
25、
26、

[image]

如果您不幸遭受警察盘问，请牢记一个首要的且至关重要的原理，那就是：如果审讯者手握无懈可击的定罪证据，他们就压根不用费劲去盘问您了。您今天坐在这里的关键原因是：条子没证据。

当警方接近您时，您应该拒绝接受问询，并立即要求律师到场，在任何问话开始前声明您的权利。

在理想状态下，根据既定法律，此时所有问询就可以终止了。但现实中警方经常施展更狡猾的伎俩，诱使您主动配合问询或透露信息——这些信息能推进他们的调查目标，却对您这个嫌疑人来说几乎毫无益处。

一旦您行使了律师在场权，无论问题听起来多么无害，都要坚持绝不回答任何提问。无论多么想回答，无论您认为问题多么无害——都要坚持绝不回应！米兰达警告已经清楚的表明了这一点：您所说的任何一个字都可能在法庭上成为不利证据。任何微不足道的自证其罪言论，都将被富有想象力的侦查人员解读为重大认罪，并被用于指控您。这是无需质疑的事实。

[image]

返回 - 镇压手段：[image]对证据的偏见性解读

审讯您的条子永远不会为您着想！不要上当。切勿提供任何可被利用的材料，仅需提供基本统计性个人信息：姓名、年龄、住址、出生日期及身份证号。关于您不得不提供的信息请查阅您本地的法规。

[image]

只要他们审问您，他们就是您的敌人。这点一定要牢记。不论他们戴上什么面具假扮什么角色，绝不可信任他们说的任何话、绝不主要动透露任何信息！

只要坐到了那里，要么您本人就是“嫌疑人”，要么您的亲密朋友或同志是嫌疑人，要么他们正试图收集情报以便将来对您或您的所有的至亲至爱不利。条子最不关心的就是您作为个人的切身利益，他们只是在履行政府指派的镇压职责。

切勿惊慌失措，更不可被虚假的安全感所迷惑。无论审讯持续多久都保持沉默，不要被时间拖垮意志 —— 要有心理准备，消耗战是老练审讯者惯用的战术。

认清他们的把戏，明白他们的唯一职能就是把您关进监狱，毁掉您的人生，让您的亲朋好友承受痛苦—— 有时长达数月甚至长达数年！

保持沉默。只要您看起来更硬更难啃，迟早他们会彻底放弃审讯，转而寻找意志更薄弱的人加以操控，使其遭受长期监禁。

审讯有两种必然结局。要么审讯结束后，您将获得自由，得以重返家人、朋友或战友的怀抱，成为历经火炼的更睿智、意志更坚定的战士；抑或，被锁入牢笼。如果遭到收押且您始终保持沉默，请在获准拨打唯一电话后抓住任何机会立即联系保释援助或律师。您的律师会很高兴有您这样一位保持缄默、未作供述的委托人。

正因您明智的沉默，律师方能施展法学院传授的魔法。如果您被指控犯罪，律师或许能在预审时以证据不足为由争取撤案。但如果您自己说出来了，就别指望证据不足能撤案了。倘若存在其他不利证据（比如最傻的错误：忘带手套了），保持沉默也能让律师有机会拓展辩护策略空间。

[image]

返回 - 自卫措施：[image]被捕支援 ；[image]镇压应对措施 ；[image]突袭应对措施

绝不放弃！绝不背叛！不要让嘴巴把自己送进监狱。捍卫您的权利。记住任何时候您都有权保持沉默。面对冷峻的法官和吹毛求疵的暴怒检察官时，千万别说出日后会让您或朋友在法庭上后悔的话！

[image]

接下来将揭露一系列警方很可能对您施展的拙劣心理战术—— 谨记：条子们总会用花言巧语诱导您张嘴，声称“坦白能洗心革面”，“让内心获得解脱” —— 都是狗屁。他们一转眼就会嘲笑您，歪曲您的所作所为，把您当成谈资鄙视您“天真愚昧”，他们享受成功操纵您的成就感。

而您只会被扔进一间污秽荒芜的牢房。那里弥漫着汗臭和排泄物的混合气味，陈腐的烟味与绝望交织在一起，而您的狱友尽是些来历可疑之徒。如果未能立即保释，您可能不得不为了餐盘和坐卧位置而展开战斗；甚至需要竭力守护鞋子、衬衫或外套，免遭社会犯人的掠夺。您不得不在众目睽睽之下排泄，遭受您可能现在难以想象的羞辱。在监狱里，您可能被迫第一次真正体会到何为“坚守阵地”——无论是字面意义还是隐喻意义。您可能被迫捍卫自己的性取向，抵御性侵犯者的侵害；也有人被迫暂时转换性偏好，因环境所迫成为双性恋者以求在监禁中保全自身。呼救是没有用的。除非遭遇极端暴行或双方冲突，否则无人会回应您的呼救 ——那些宣誓保护民众的执法者，通常对囚犯视而不见。

一旦被登记 **[image] 指纹** 、被关进牢房，切勿向周围任何表现出好奇的囚犯透露任何案情！每个愿意听您诉苦的囚犯都可能成为法庭上的潜在威胁——他们要么是监狱线人，要么是与您同牢的卧底警察，其唯一目的就是取得信任并诱使您认罪。您可能成为被盯上的目标，认清这个事实，闭嘴！经典案例发生在1980年代初：田纳西州囚犯加里·哈特曼向狱友雷蒙德·弗雷泽透露了自己参与的一桩谋杀案。弗雷泽联合另一名囚犯肯尼斯·金，在狱方协助下联系总检察长办公室和执法部门，领取了1000美元悬赏金，哈特曼最终被判死刑。历经十余年死囚牢房后，哈特曼的死刑判决在上诉中被推翻，改判终身监禁。

正如一战二战时期的警句：言多必失。

[image]

以下是警方诱供时最经常施展的心理战术。

务必透彻了解对手，识破其手段及其无数变体 —— 这些手段多种多样如同被审讯者与审讯者的性格般千变万化。

[image]

您能否保持自由，终将取决于您的意志力与对审讯战术、施压手段及心理压力的认知。

每种手段都旨在诱发被审讯者的特定反应。

1、

审讯者常以“你还有什么可反驳的？” 的姿态，表现出对嫌疑人罪行的笃定。

而您，应该为对手毫无证据这一事实，表现出更高的笃定。

2、

审讯者仅列举部分（绝非全部）指向嫌疑人罪行的间接证据。这实为“我掌握的信息远超所言，如果你的供词与我掌握的情况不符，你就完蛋了” 的变体。

事实上多数情况下审讯者根本就一无所知，因此会抓住您提供的任何信息加以利用，反向利用并抛回给您以获取更多情报。

3、

审讯者常常刻意关注被审讯者身体或心理的异常表现 —— 颈动脉搏动、喉结过度活动、回避眼神接触、抖腿、搓手、手指敲击、抠指甲等等个体化的紧张小动作，都是人在压力下的生理反应。也是赌场里的老玩家都熟知的常见“破绽”。

如果嫌疑人情绪波动，审讯者便会引导其关注“内心异样感受”，利用道德愧疚感诱导认罪。

4、

审讯者常通过 “我可能也会这么做”、或者 “任何处境相似的人都可能采取同样行动” 等类似话语假装同情，试图塑造 “盟友” 形象 —— 在敌对环境中营造可被信任的氛围 ... 但其目的只有一个，那就是，让目标对象接受这种欺骗性联结，从而坦白自证或牵连他人。

如果您能牢记审讯者与您之间亘古不变的永恒敌对关系，就不会让自己上当受骗。

5、

审讯者常在问讯中通过特定措辞减轻被审讯者的罪恶感，尤其在涉及所谓的暴力指控时，刻意淡化罪行的严重性。例如：“我很理解你啊，换任何人遭受这种情况都会做出同样的事”、“如果有人这样对我，我也会跟你一样做出同样的事！” 千万不要搭理他们。

6、

熟练的审讯者可能为被指控的罪行暗示一种较不令人反感、更具道德合理性的动机或理由，而非预设的原有动机。这只是为了让您放下恐

惧，坠入他们的陷阱。

7、

为瓦解被告意志以获取供述，有经验的审讯者经常通过以下方式对嫌疑人假装同情：(a) 谴责受害者 —— “那种人纯属活该”；(b) 谴责任何可能或已被指控的共犯嫌疑人 —— “就是那个家伙连累了你”；(c) 谴责任何可能被认为对该罪行或已指控罪行负有道德责任的人 —— “你被那种人害惨了。而我可以帮你，前提是……”。

8、

审讯者假装理解和同情，通过肢体接触 —— 比如如轻拍您的手背或肩膀、握住您的手 —— 来敦促您认罪，随后常伴随着审讯者的宣称：倘若他的母亲、父亲、兄弟、姐妹、妻子、子女、女友、同性伴侣等被指控犯下这样的罪行，他会“...劝他们认罪...”，“... 说出真相...“。

审讯者常援引道德概念，比如 “认罪是唯一体面而光荣的选择"、“你该解脱良心负担，了结此事才能心安...”，云云，试图建立情感纽带，尤其针对那些经历多次长时间密集审讯、在轮班审讯员持续逼问下遭受精神摧残的受审对象。

臭名昭著的“好警察坏警察”或友善/不友善套路，通常在其他伎俩失效后启用 —— 当假惺惺的同情与理解策略屡屡碰壁，条子们懊恼不已时，这套戏码便会登场。您肯定在影视剧里见过那套老掉牙的“好人坏人”套路，那不是虚构的。然而悲哀的是，对于遭受长期心理摧残的人来说，这类戏剧化手段往往就能奏效。

9、

老练的审讯者还经常采用双重策略：或者暗示控方存在夸大成分，或

刻意渲染指控罪行的性质与严重性，以此震慑被审讯者使其作出“辩解陈述”—— 试图解释“真实经过”，最终却在自掘坟墓中彻底自陷囹圄。

此等伎俩堪称双重“蠢”。

10、

审讯者会引导被问询者假设性地置身于所谓的犯罪现场，设想其与引发犯罪的事件存在某种关联，以此来获取信息、诱使对方不经意间脱口而出认罪供述。

11、

如果受审者天真地承认曾现身案发现场，审讯者便会要求其反复复述事件经过，借此来捕捉叙述矛盾点，进而指出矛盾之处，迫使其承认对某些细节或犯罪行为撒谎。

每次诱导出的认罪都会加深受审者的 心理脆弱性 ，使其更易吐露“全部真相”。

12、

审讯者常通过精心挑选的奉承之辞或直接挑战荣誉感来诉诸被审讯者的自尊心，利用人类追求他人认可的基本心理需求，通过刺激你来围猎你。

13、

反复强调抵抗是徒劳的。装得好像他们有权当晚就枪毙您似的。

14、

老练的审讯者会反复强调嫌疑人“持续否认犯罪行为”的严重后果。这种说辞对怀有正义感的政治动机嫌疑人完全无效，注定失败。但对社会犯罪嫌疑人往往奏效—— 因其犯罪生涯中，许多惯犯曾闪现过自我改造的念头或意图。

15、

有时审讯者不直接要求嫌疑人全面认罪，而是先就犯罪细节或动机提出疑问，佯装困惑地追问“为何作案”？

这不过是利用 自白冲动——当审讯持续越久，这种冲动就越强烈 ，对年轻人或缺乏经验的人来说尤其如此。

16、

如果前述审讯手段均告失败，或预判实施后仍将失败，审讯人员就很可能会 开始挑拨您和队友的相互对立。

他们把您和其他人分开审讯，并告知其中任何一人（或多人）说其他被审讯者已经招供。

审讯者会要求当事人“趁他/她/他们把你当替罪羊之前赶紧说清楚！”；或者 “你太蠢了还在帮那人守口如瓶！而那个家伙都已经出卖你了，不如老实交代！”

此类手段常伴随愤怒的手势和恐吓。

如果受审者显露软弱，则会得到虚伪的同情。

[image]

采取直接行动时务必认清同伴！行动前务必统一口径！守口如瓶！

彼此依靠，信任彼此始终依靠，就不会上当受骗 。

这是获取供词的经久不衰之法，理智的被告本不该上当。针对政治动机的嫌疑人，分而治之的策略成功率虽低，但仍偶有奏效。

[image]

返回：[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

17、

审讯者会通过询问嫌疑人是否知晓“为何”被问询，诱使其承认对案件知情。

当受审人主动透露所谓的犯罪细节时，往往犯下致命错误 —— 这些信息唯有犯罪者或现场目击者才可能知晓。

此类认罪陈述虽有助于调查（因审讯者可据此锁定犯罪主犯、共犯或证人），但最佳策略是除必要身份信息外保持缄默。

申辩清白只会开启与审讯者的对话，这种情况下任何对话都只会对被指控者不利。

18、

审讯者通常先要求被审讯者陈述其对受害者及其他潜在嫌疑人的全部了解，继而才进入具体事件/违法行为/犯罪行为的询问。

对多数被审讯者而言，一旦开口往往难以停下，远比始终保持沉默更困难。人类天生热衷于谈论并试图用所知所学在任何话题上博取他人赞赏。

不会装傻在很多情况下都有危险！

19、

经验丰富的审讯者会竭力获取嫌疑人犯罪前、犯罪时及犯罪后的详细活动轨迹。

监视摄像头 、 目击者 、 **DNA** 、 指纹 和 智能手机 等等所有信息都会暴力一个人的行踪。 不遵守 **[image]** 数字技术限制和最佳实践 的行动无疑是亲手给自己挖坟。

20、

当警方审讯员已掌握犯罪事实时，常会以漫不经心的语气询问这些已知情报 —— 佯装当局尚未知晓真相 —— 以此扰乱嫌疑人神经，使其更易受激进审讯手段影响。

此举旨在让嫌疑人怀疑其他涉案人员已供认不讳。恐惧、猜疑与不信任交织的情绪风暴，已将朋友、恋人、伴侣与家人彼此对立。

[image]

如果审讯者能通过挑拨离间获取供词，他们必将乐此不疲 —— 摧毁友谊、背叛信任、瓦解家庭！您的亲友乃至你自身，在他们眼中不过是废弃的厕纸。

若能洞悉此理，您便已领先于那些受压迫心理战术所惑之人！

[image]

在示威现场如果存在暴力镇压的丝毫可能，务必紧贴可信赖的同伴，以防被警察突然抓捕！

如果遭逮捕或集体被捕，请信任您的亲密队友，相信你们彼此间的保护胜过一切。

行动前做出充分的 [image] 镇压应对措施 和 [image] 被捕支援 措施，确保有支援者能在您被押往监狱时帮您联系保释担保人或律师。

如果是集体被捕，人数就是精神力量，你们可以集结资源共同脱身。

参加示威或者及其他直接行动时务必结伴可靠友人，孤军奋战本身就是巨大的危险。所有直接行动务必只携带经受过考验的铁杆伙伴！险境之中绝非是试探忠诚的时机。

审讯中要意识到战友的力量 —— 闭上嘴，压制任何开口的冲动，更不要承认任何罪行，否则就是在主动成为监狱人口统计数据。

21、

审讯过程中，条子有时会间歇性地向受审者询问他人的情况，其提问方式是暗示正确答案“早已知晓”。

例如这样问“你认识李大锤多久了”，而不是“你是否认识李大锤”。

另一种伎俩是在提问前先警告对方“你仔细想好了再回答下一个问题”，意在给您的神经线加一层紧箍咒，而该问题本身与罪责认定并没有直接关联。这是在条子自认为把握住了您的基准线后测试操控您情绪的便捷程度。

此类手法最常出现在负责审讯的条子翻阅文件的时候，或者其手持文件对您进行提问的情况下，并且在您回答任何问题时立即流露出怀疑的神情。

这种提问本质上是在诱导您作出辩解性回应。无论您认为对方是否已知晓答案，都切勿作答，您应该完全无视此类问题。

22、

审讯者可能提及某份并不存在的“罪证”，借此来观察受审者是否试图辩解。

如果受审者作出辩解，则暗示其有罪 —— 因为有罪的人才会在掩盖行踪方面提心吊胆，而无辜者无需掩盖行踪，自然不必揣测罪证被发现的可能性。

您是无辜者，您当然应该大大方方。

23、

经验丰富的审讯者会询问被受审者是否曾“考虑过”实施正在调查的所谓罪行或类似行为。

如果受审者蠢到回答此类问题，审讯者很可能会在法庭上作证称您“曾吹嘘或夸耀过犯罪念头”。

您应该响亮的回答“ 没有！ ”

这才是无辜者的典型回应。

如果您失言承认，下一个逻辑问题必然是：“这种念头最终让你在最

脆弱的时刻——承受巨大压力时——屈服了，对么？我能理解的。你仔细说说吧。”这就是诱供。

24、

在涉及破坏公物、毁坏财物或盗窃的案件中，审讯者会试图诱使受审者提出赔偿方案 —— 这正是认罪的重要信号。

当提及赔偿时，无辜人的正常反应应该是明确声明：绝不为未犯之事或未窃之物买单。而警方真正想诱导有罪者说出的话是：同意赔偿受害方的损失，紧接着再声明自己与破坏、毁损或盗窃行为毫无关联。此时受审者已将自己置于死胡同了。

25、

受审者常被问及是否愿意接受测谎？无辜者几乎总会立即同意接受任何测试以证明清白。有罪者则倾向于当即拒绝测谎，或在同意后找借口推脱。

事实上，测谎很少作为调查工具，警方只能依靠现有资源 —— 即借助电子设备辅助的、基于常识的熟练审讯技术——来锁定嫌疑人。如果您同意接受测谎，99.9%的情况下，对方提出测试不过是烟幕弹、虚张声势或试探您自证清白的意愿。精明的人反而应在这类情境下主动要求测谎。目睹权力机器的退缩姿态，或许还能获得几分滑稽的解压效果。

[image]

返回 - 在这里看到对付测谎仪的方法：[image]如何欺骗，和如何防骗：反侦基础课 S06E07

26、

在涉及激进派直接行动的案件中，如果受审者看起来很愿意配合，但只是拒绝承认与案件有关，这种状况在条子眼中相当于“嫌疑极大”、“应该加刑”。

[image]

审讯技巧的种类比警察还多。前文所列举的仅是其中最常见的、最可能常用的几种。

对于应对警方审讯的最佳建议总结成一句话就是：如果对方无视您坚持要律师在场的请求仍坚持审问，请务必全程保持沉默，对所有提问拒绝作答！

切勿主动提供任何信息 —— 无论您认为多么无关紧要或微不足道，也不要说，切切 —— 因为您可能在不知不觉中提供了关键线索，正是这块拼图使他们得以起诉您或他人！

不要自以为是。始终牢记敌对关系 —— 不论审讯场景被营造到多么“融洽温馨”，始终牢记坐在您对面的是劲敌，其背后有着比您强大一万倍的镇压系统撑腰。有些受审者虽然不容易被话语操纵，却容易被气氛所操纵，甚至幻想着自己能“掌控对话”。千万不要。您绝不可能从警方口中“套出”任何信息，倘若他们能给您一个字的实话，就必然要从您口中得到一千字的实话。他们是专业专职干这个的，而你我都不是。

[image]

简言：保持沉默、缄口不言、自由自在。

就算被起诉，行使沉默权也将为您赢得案件提供最佳机会！

愿天下所有勇于反抗的兄弟姐妹好运！祝福大家永远不要身陷本系列的语境下。被审判的应该是我们的敌人。 保持沉默，就是保持自由！让他们永远抓不全我们！

[image]
[image]

如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04

[image] 关键词	审讯心理学 心理安全 逮捕
[image] 关联	[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛 ；[image]被捕支援 ；[image]镇压应对措施
[image] 创建时间	2025年3月5日
[image] **Description**	心理安全；反渗透和协作

被捕和牢狱并非完结。它只是我们漫长的反抗斗争中的一个环节，尽管可能是最糟糕的环节。所以我们需要更大的智慧以便更平安地渡过难关。不要被摧毁。

不要被操纵。要全须全尾地取得胜利。

- Table of Contents

  认清处境
  被捕
  在监狱里
  庭审准备
  出庭受审

[image]

本集内容献给所有因参与正义事业和解放斗争而面临监禁的人。同样适用于任何投身此项斗争、其行动可能与统治制度的法律体系这座庞大惯性建筑发生碰撞的人。

我仅能基于自身经历发言。但愿我与司法体系周旋的这部分经历能对未来者有所启发。我并非律师或法律专家。本文初稿发表于2004年[收录于《灾难食谱：无政府主义者手册》]，当时的处境与现在不同，更不会保证与未来一致，不论您什么时候读到它，请务必保持审慎态度。

但是请相信——无论您是谁，我的心与您同在。

您并非第一个经历此等困境的人，也不会是最后一个。你的反抗斗争属于一个悠久而光荣的传统，它横跨全球，纵贯古今。

我知道眼下形势严峻。我自己也曾如此。感谢你曾作出的英勇之举。你并不孤单。你能应对这一切。

认清处境

糟糕。出岔子了，你现在惹上了大麻烦。所有迹象都指向一个不可避免的结论：事情会发展得很不顺利。你害怕极了。你肯定没想到事情会变成这样。谁来喂咱的猫？下周五还得交房租。现在可不能进监狱啊。到底会发生什么？……

好了。保持冷静。在处理眼前状况前，先深呼吸几次，后退几步。

首先要明白：无论是法律手段还是非法手段，镇压都是革命活动的必然结果。若想完全避免，唯一的办法就是挂起你的佩剑，停止挑战这个疯狂的世界秩序。你心知肚明，若真如此，你将无法在晨光中直视镜中的自己。况且对某些背景、经历和肤色的人而言（或许就包括你）即便对现状完全屈从，也未必能保证免受其怒火。

掌权者的逻辑很简单：他们需要树立典型。他们要杀鸡儆猴："看吧？这就是越界的后果！你不想遭遇同样下场吧？那就老实点！”而你我就是那只“鸡”。

这种负面强化是一种明智而有效的策略。它自古有之，在有限范围内效果显著。

有时人们确实会放弃抵抗，屈服于失败主义与愤懑的重压。特定情境下，有人甚至会在压力下崩溃并相互倾轧。有些灵魂就此被摧毁。

遭受酷刑时，几乎任何人都可能做出任何事。我对此略知一二。但其必然结果是：压迫迫使我们团结起来，我深信这种策略最终往往催生出比它摧毁的更多的抵抗力量。

话虽如此，在制定计划时，你最好了解一些基本准则。行动越积极，最终遭遇法律机器的可能性就越大。你的行动越有效、越激进、越鼓舞人心，这种遭遇就越可能变得格外不愉快。一场严肃的刑事审判绝非乐事 —— 它令人恐惧、耗时费力、代价高昂且充满危险。无论从事何种行动，被捕受审都是潜在后果，但这应尽可能避免，而非追求的目标。制定行动方案时，最大化效果同时最小化风险才是明智之举 BACK 周密的行动计划 。我并非主张遵纪守法，而是强调行动价值取决于其有效性而非违法性 —— 切勿混淆二者！

如果你决定实施违法行为，务必事先坐下来仔细推敲可能触犯的具体法规，并预估违反这些法规的最高刑罚。冷静自问：若事态发展至最糟境地，你能否承受其后果？如果答案是否定的，请务必远离深渊，另寻他途。这绝非耻辱。虽不愿如此直言，但若无力承担刑罚，那就切勿触犯法律。

如果答案是肯定的，再提供几点建议：与其盲目闯入可能导致被捕的境地，不如预先制定应急方案。提前与律师建立联系，明确紧急联络对象及具体行动指令。若条件允许，预留保释金。

祝你一路顺风，好运相伴。

[image]

返回 - 自卫措施：周密的行动计划 ；[image]镇压应对措施
；[image]被捕支援

[image]

被捕

无论如何，这一切对你而言都已成为过去。我无从知晓这篇文字会在何时送达你手中，因此，我将从上次中断处继续 —— 从开端说起。

此刻你正坐在警车后座，心怀恐惧。

当下你最该做的就是：绝不与警方交谈。一个字都别说。无论你做了什么或没做什么，都无关紧要。无论你是否被当场抓获、抑或正遭受牵连至国际权力最高层的构陷，都绝不能开口。

你只需说：

> “我将保持沉默。我要见我的律师。”

除此之外只字不提。这点再怎么强调都不为过。如果你只能记住本文中的一句话，那就该是这句话：

> “我将保持沉默。我要见我的律师。”

即便他们试图用任何不想干的话题跟你套话，你也只能重复上面这句。

即使他们把你的头往墙上撞，你仍只能重复什么这句。

当“好警察”佯装善意声称要帮你的忙，“坏警察”却突然逼近你；当他们威胁要把你关进连环强奸犯的牢房，扬言让你后悔活着，声称你的朋友已经告发你且他们早已掌握了一切； 如果他们踢你打你、猥亵你、拖你走、断你食水、剥夺你的睡眠和医疗，如果他们剥光你衣服用冰水浇透你，或者关紧窗户调高暖气，将你铐在椅子上任你尿湿便

秽，你仍只能说这句话。

无论他们说什么做什么，你必须说：

“我保持沉默。我要见我的律师。”

除此外只字不提。

只要你失言开口，每个字都将在法庭上成为你的罪证。

只要你能挺住保持沉默，他们终将放弃。

你将被关押在某地警局或分局。逮捕后约四十八小时内，你将接受提审。这是刑事案件中你首次出庭受审。届时将正式指控罪名，如果你尚未聘请律师则会为你指派公设辩护人，你需作出有罪或无罪答辩，并根据指控严重程度及其他因素决定是否准予保释。

无论最终采取何种法律策略，此时都应坚持无罪答辩。

请尽快联系亲友，要求他们着手为您聘请律师并办理保释事宜。

[image]

在监狱里

提审结束后，你很可能会被转移到地方拘留所。这里通常关押着等待审判的人、服刑期较短的囚犯，或是正在服完监狱刑期的囚犯。你会得到食物、热水澡，最终被安置在普通囚室。尽管你可能不愿承认，但淋浴的感觉真的、真的会让你舒畅无比。

在此你将不得不适应眼前世界的两大群体：囚犯与狱警。很快你就会发现，狱警堪称地球上最粗鄙、最满口脏话、最擅长言语霸凌的物

种。如果被关押在男监，你随时可能被命令"撩起蛋蛋！掰开屁股！”，时刻被告诫“耍娘娘腔就让你吃不了兜着走！”，还要忍受满天飞的“婊子养的！”“基佬！”之类的污言秽语。

这些大多是故意激你发火——如果你显得敏感脆弱，他们就绝不会罢休。

[image]

切勿公然敌对、更不要给他们找到揍你的理由 —— 他们真会动手。

也别畏缩、卑躬屈膝或表现得过于顺从 —— 那绝非良策。

保持礼貌，莫露半点软弱。

待他们对你失去兴趣后，日子就会好过些。

囚犯与狱警的关系复杂而诡谲。观察下就能发现其他囚犯们那些微妙或不那么微妙的手段——他们总能恰到好处地削弱狱警的权威以获取所需，却又不会招致暴打。但你自己效仿时务必极其谨慎，尤其当你是新来的，就更要小心 —— 因为这种情况下你不被看作是被监禁阶层的一份子 —— 后者在“顶嘴”方面会得到一些宽容。隔壁的家伙能敲着牢房外的杯子大喊“狱警！狱警！他妈的给我拿点水来！操！”这不一定意味着你也可以。

监狱在各方面都充满悖论。首先，你越富有、种族地位越高，司法系统对你就越宽容，但其他囚犯对你的态度就越恶劣。你的处境取决于肤色、举止和言谈。无论如何，你必须表现得体。你需要用简洁明了的方式解释自己，让狱友们能感同身受。这项能力比任何其他因素都更能提升你在狱中的生活质量。切勿摆出愤慨姿态、不要喋喋不休申辩清白，更不要抱怨牢骚。总有人比你更惨，每个人都遭遇过不公，没人想听你的悲情故事。

许多囚犯对安全意识的彻底缺失会令你震惊。你会听闻各种离奇的故事：同牢房的武装抢劫犯如何逍遥法外，他如何策划从芝加哥线人那

里搞到海量冰毒，又如何在他奶奶家床底下的鞋盒子里藏着杀过人的枪 ——只盼着检察官别在小兄弟来取货前拼出真相。当然，这些话大半是吹牛的，但其中不乏真实成分。天啊，千万别参与这种蠢事。

[image]

要是当局真想抓你，随时都能向你身边的人施压，查探你是否说出过什么。

如果你真的泄密了，那就等于替条子干了活，法庭上自会见分晓。

如果狱友拉闲话说，你只需陈述被指控的内容 —— 已经在案卷上的那些 —— 除此之外的都不要说。想谈政治立场尽管谈，但别扯你自己的案子。

各地规定不尽相同，但通常在被捕后约十天内，你应该可以获得初步听证会或大陪审团听证会。这是对指控的初步审查。检察官必须提交证据和证人，证明所谓的“犯罪行为”确实发生，且存在合理理由相信“是你”实施了该行为。这一法律门槛远低于定罪所需的“排除合理怀疑”标准。

这场听证至关重要，因为这可能是你唯一能提前接触部分检方拟在庭审中使用的证词和证据的机会。

你无需在此阶段作证或提供证人证据——通常也不应如此，因为这只会让检方听闻你的陈述并准备反驳。如果法官认定存在合理依据——通常他们都会这么做——你将正式被起诉，并确定庭审日期。

服刑期间要掌控自己，别被环境吞噬。阅读、写作、锻炼、冥想，做任何能让你保持专注和积极的事情。尽量别看电视。

你身处的世界已彻底崩坏，但这并不意味着所有囚犯的互助本能都被扼杀了。你会逐渐发现囚犯们互相照应的种种方式。比如你的狱友A，正把回形针插进墙壁插座以引出火花来点燃大麻卷。你会看见那个混蛋狱警B突然走过来，刚好让你来得及提醒狱友把大麻藏进床垫

里。待狱警B离开后，A会说“多谢关照，多谢关照”——这句行话意为“我们身处险境必须互助求生，你尽了本分，我心领了”。你甚至可以从周日互相搂着胳膊谈论死亡幽谷的那些人身上学到东西，也能从朝向麦加叩拜诵读晨祷的穆斯林身上领悟真谛。我虽不崇拜有组织的宗教，却明白他们谈论的内容与缘由。

倘若我们这些具有生态意识的反权威主义者终将能为文明的死亡行军踩下刹车，必将目睹大批同道者身陷囹圄。

历史上所有革命运动都曾面临此境。虽非我亲历之事，但我们必须找到在监狱体系内延续斗争的途径，使监禁不再是个人政治道路的终点，而仅仅是发展历程中一个虽不愉快却可接受的阶段。纵观全球历史，从朗凯什到库尔德斯坦，从阿提卡到哥伦比亚再到西雅图，此类先例比比皆是。

[image]

就连监狱帮派在此方面也颇具启示意义——它们在许多监狱拥有足够势力，以确保其成员获得相对优待。

如果能建立这样的狱中 接应网络 ，将极大缓解囚禁带来的恐惧，而我们这些在外面的抗争者也将更有底气行动。

请为此尽己所能，但切记：目前我们离目标仍遥遥无期。

比我更久居牢笼者或许能更细致地描述狱中的生存之道，但只需知晓：监狱确是人间地狱，尤其当没人认识你、没人为你撑腰时。殴打、刺杀、强奸、甚至谋杀 …… 皆在所难免。

因此尽可能让自己的体格壮实些、懂点格斗技能肯定没坏处，但别搞错了：真正能助你生存的不是胳膊大腿，而是你的嘴巴和你的头脑。我并非鼓吹你耀武扬威证明自己够狠。我的意思是：你必须以正直的姿态赢得尊重，通过体现你为人民为土地而战的姿态，像你本应成为的那位谦逊而勇敢的战士一样，来赢得尊重。

[image]

一旦在铁窗后度过些许时光，你将获得若干直击灵魂的领悟。首先，囚禁野兽是践踏捕获者与被捕者双重精神的可憎行径—— 倘若“原罪”一词尚存意义，此举便是致命之罪。

你将有足够时间反思所陷体系的彻底虚伪 ——它如何滋养人性中最恶毒暴戾的本质，如何制造、摧毁、生产、消耗、培育并释放那些赋予其永恒生命的怪物。监狱造就杀手，杀手滋生监狱，而从这场病态闹剧中牟取暴利的富人混蛋们，正笑嘻嘻地数着钞票走向银行。

如果你是男人，且足够明智，你会思考每时每刻都处于性暴力迫近的危险中是什么感觉，并思考那些不得不一直应对这种情况的女性经历着怎样的煎熬。如果你是白人，你将窥见身为弱势遭受威胁的少数族裔的滋味，体会到有色人种时刻承受这种处境的煎熬。

你会发现，当“同意”的伪装被剥去，整个处境在某些方面反而更显赤裸。这里只有纯碎的暴力，无人掩饰其本质。无论你是否情愿，都必须服从指令，否则就会受伤。

你会意识到生命中蕴藏着无限可能 ——一天、一小时、一分钟、一周、一月、一年、一生。你会惊叹于那些平凡的日常何其珍贵：漫步在破败的城镇，与朋友闲坐，和母亲闲聊，弹奏吉他，在某人怀中入眠，自慰，做爱，哭泣，抚摸猫咪，烹饪，徒步，驾车，睡到自然醒；凝望日头、月亮、星辰、天空、树木、飞鸟与松鼠；感受火焰、雨水和风的触碰。你将无法理解自己曾如何视这些为理所当然。在某种你不舒服、不骄傲的层面上，你会觉得自己像个傻瓜，竟然拿自己的自由去冒险：无论你所做的事情多么紧迫、必要、勇敢和高尚，与你所失去的一切相比，都会显得微不足道。你会发誓，你将绝不再让任何一天白白溜走，你会榨干每一分钟的所有价值，对能够活下去这一恩赐心存感激 —— 你将永远不会忘记此刻这份令人心碎的、想要活下去的渴望。

若终得出狱，这份感受终将褪去，但你总会重拾它，或它自会寻你而来。若未能出狱，你将以最痛苦的方式领悟：生命价值的源泉深植于你的内心，无人能夺走，无论流落何方皆随身而行。

无论哪种结局，你都将不再是原来的自己——或更加坚韧强大，或彻

底破碎。

但愿某天你会获得保释，尽管如果罪名足够严重或保释金过高的话，这未必能实现。无论谁出钱或如何筹措，务必确保保释金仅以你个人名义缴纳 —— 如此即便你最终成功潜逃，他们也无法让你的亲人倾家荡产。

倘若那个方脑袋的大块头狱警真来通知你回家，你将目睹一个滑稽的场面：牢房里每个凶悍的重刑犯都会跑来抢夺你的纸张、铅笔、牙膏、枕头、毛巾、毯子、泡面、指甲钳以及所有值钱物品，他们笑得像圣诞节的孩子，真心为你高兴，又雀跃着看你离开。同号的狱友会逼你发誓替他抽根粗壮的大麻卷，还得你替他联系外面的某个小兄弟。

当你终于踏出监狱沐浴阳光时，那感觉堪称人生至臻时刻——可某种意义上，出狱比入狱更难熬，因为一旦重获自由，你便害怕再度沦陷。

[image]

庭审准备

我想，现在是时候提出一个最令人烦恼和恼火的话题了，那就是 —— 你的律师。即便在最理想的情况下，你与这位人士的关系也可能比其他任何关系都更令人抓狂又沮丧。在最终确定陪你出庭的律师之前，你可能要经历多位律师的更迭。提审阶段仅需公设辩护人即可，但预审听证会召开时你必须着手正式聘请律师。

那些心怀善意的活动家 —— 顺带一提，他们自己并不面临刑期 —— 会急于为你推荐各类富有同情心的“维权”律师，而这些律师很可能令你的法官反感。我并不是说律师在政治上对你有同情是任何坏事，但这绝非你的首要考量。

[image]

所有律师，包括所谓的维权律师，本质上都是雇佣兵。你身边朋友多的是。但这种这种情况下你需要的不是朋友，而是枪手。

所以你的首要考量绝非是律师的政治立场 —— 尽管你当然不该选个法西斯来做辩护律师 —— 而是此人的庭审战绩、过往表现、与法官检察官的关系等。

身陷这般险恶的小世界固然可悲，但既然身在此中，就该按规矩行事。此刻绝非胡闹之时。

你和团队必须竭尽所能搜集证据，聘请力所能及的最强律师。

显然，越是穷困潦倒，越会被当权者彻底玩弄于股掌之间。必要时向所有熟人借钱。没错这简直糟透了，但这就是制度的运作方式。

若面临重罪指控， 你需要找那种深谙权谋之道、曾成功救人脱离死刑的律师。

其他好心的活动家会告诉你：该把司法体系告上法庭，该自己为自己辩护，该把庭审当作政治论坛，当庭谴责资本主义和专制制度，该表现得疯狂些，等等等等。那些关于向权力说真话的和平主义言论自有其时宜场合，但我建议你在决定面对地区检察官、法官和法庭速记员发表演说前，好好斟酌一番。法庭上的怪异举动通常只适用于两种人：一是面临指控不甚严重、损失较小者；二是明显遭受冤枉或按法律标准无可辩驳的罪犯 —— 此时出其不意反成最合理的选择。当然，此类策略偶有奏效，但终究是特例。MOVE（Move Out Victoriously Everywhere）组织的抗争便是例证——他们无畏坚韧地与法律对抗，屡屡取得胜利。若选择这条路，就必须义无反顾，且务必做到极致。

整个司法游戏充满冷酷算计。国家机器的目标是竭尽所能将你长期监禁，而你的任务是在不背叛任何人的前提下洗脱罪名。

[image]

若有共同被告，你必须与他们建立牢不可破的纽带 —— 任何手段都无法瓦解的纽带。

在每个环节，国家机器都将不遗余力地挑拨你们相互猜忌。

同舟共济方渡难关。此理不言自明。

切切切记：绝不可牺牲他人以求自保。不可与检方合作，不可接受污点证人交易。

如果存在共同被告，最佳策略是达成共识：未经全体同意不得接受任何认罪协议。如果面临刑期差异悬殊的情况，则处境最危者拥有最终决定权。

务必让律师明确知晓此立场。切勿幻想雇佣枪手为己方辩护能带来任何东西。

你的律师绝不会对损害共同被告、同伙、运动组织或其他非付费方的利益有所顾忌。律师们常为那些互相残杀的无良之徒效力，这在他们圈子里是常态。务必明确表示这种行为不可接受。除非律师是彻头彻尾的混蛋，否则他/她理应对你的这一做法心存敬佩。

随着案件推进，你会发现一个令人抓狂的事实：你的烦恼对你而言远比对律师而言重要得多。当你急切地想要打探十天后听证会的关键消息时，对方却可能整周泡在另一个地方，忙着处理两年前某人抢劫酒铺的案子。律师手头还攥着一堆可怜虫，每个都和你一样走投无路。但这属于他的麻烦，与你无关。吱吱作响的轮子才有机会得到润滑油，你必须竭尽全力确保自身需求得到满足。如果你太顺从了任由他们将你扫到地毯底下，他们就肯定会这么做。如果你持续被关押，情况就会加倍棘手。打电话、打电话、再打电话，必要时亲自去办公室。对秘书们要极其客气和尊重：他们掌握着通往城堡的钥匙。摸清办公室里各色人物的相处之道，学会找对人办事。务必避免因沟通失误错过开庭日期，否则将面临法庭逮捕令和保释金被撤销的后果。

奉一切神圣之名发誓这是最佳做法：切勿向媒体透露案件任何细节，

更不可授权他人代为发言。任何言论都将在法庭上反噬你自身 —— 请相信我。如果获保释，务必在审判前远离麻烦。

候审期间，亲友支持者会询问如何协助。这可能令人应接不暇，但你需要所有能获得的帮助。不过有些帮助有益，有些则有害。确保任何代你行事者都能对你负责，并符合你认定的最佳利益。警惕任何借你之名谋取私利者，无论其动机为何。

[image]

更难的是：若家人因恐慌而试图说服你配合当局，坚信这能帮你脱罪——务必对他们保持极其强硬的拒绝态度。这绝无可能。

切勿任人摆布，纵使对方是至亲。

切勿孤军奋战。与那些值得你托付性命的人紧密团结，让他们为你提供支持。亲友可协助筹措保释金与法律费用，寻找并研究律师资源，如果你认为有利可循则可以考虑协助宣传案件，在必要时寻找证人、证据及专家证人，如果你需要，可以在庭审和其他出庭时组织人到法庭旁听，争取信誉良好的社区成员的背书，必要时处理媒体关系，让你在精神、情感和心灵上保持稳定，以及成千上万的其他事情。永远倾听你信任之人的建议 —— 但毕竟是咱自己的脑袋放在赌上，所以咱自己最好能掌握主动权。再次强调，若无法保释，这一切都会困难得多！倘真如此，你最亲近的支持者将变得极为重要。

每桩重罪案件都是微型法律传奇，且各不相同。但无论如何，从预审或大陪审团听证到正式审判之间，你总会经历一段漫长的等待期，期间穿插着各类听证、上诉、动议及其他出庭程序。根据检方意图，地方政府既可能闪电开庭，也可能无限期拖延。无论哪种情况，过程都极其煎熬。

反复研读庭审记录和相关判例法，直至对案情了如指掌。如果仍被羁押，务必充分利用法律图书馆的每一分时间。

更可汲取囚犯群体和狱中律师们积累的丰富法律智慧。对听闻之事务必持保留态度，但仍要倾听学习。这些积累将使你更容易与律师沟

通。重申一次：向任何人谈及案件时，切记永远不要讨论你“做了什么”或“没做什么”，只谈与你在预审或大陪审团听证中“据称”所作所为相关的有记录内容。

这将是一段极其艰难的时期。牢记谁在支持你、谁背弃了你，永远不要忘记。

竭尽所能改善处境，但别沉溺于困境本身。寻找其他事情来专注，既不影响你的案件，又能阻止深渊将你吞噬殆尽。

你将反复经历极度抑郁、暴怒与否认。事实上，从被捕到受审期间，你将粗暴地穿越悲伤的经典阶段，伴随着所有随之而来的疯狂。你将恐惧重返监狱。强奸的阴影将如影随形。噩梦纠缠不休。你将成为最爱你之人难以忍受的麻烦，偶尔会彻底失控。你会嫉妒死所有能暂时遗忘的人——哪怕只是一秒钟，因为你每分每秒都不得不思考审判。你会感觉自己身患绝症。与人交谈时，你永远无法确定对方是否知晓真相。你会觉得自己是周围所有人的负担和累赘。你会试图处理完生命中所有未了之事，同时又忍不住怀疑：这是最后一次见到奶奶吗？最后一次看这片湖吗？最后一次看那棵树吗？你会厌恶那些强颜欢笑着告诉你“一切都会好起来”的人。

如果你保释在外，还会面对另外两条看似稍具诱惑的出路——潜逃或自杀。我将分别论述。

我不会断言逃亡永远毫无道理，有时确实逃走是最佳选择。当你面临恶性重罪指控，明知必将定罪，且结局注定惨烈时，逃走才是上策。如果选择此路，我愿为你祈祷。这条路永远无法回头。保持自由绝非易事，既不浪漫，也不安全，更谈不上快乐。他们会追捕你，稍有疏忽便会落网。

恳请仅在万不得已时再考虑此选项，除非你已制定非常周全的计划，已经确知余生如何在逃亡中生存，否则切勿轻举妄动。与其终生藏匿我宁愿服刑五至十年。当刑期逼近十至二十年甚至更久时，我或许才会另作打算。

关于自杀，我只能说：曾有过这样的时刻，支撑我的唯一念头是——那些对我施暴的混蛋正试图置我于死地，而我绝不会替他们完成这项“工作”。这很扭曲，但若你必须靠纯粹的怨恨维系生命，那就这么做吧。

[image]

在审判前好好活着，这样即使入狱也无怨无悔。

尽你所能善待所爱之人。

学会直面最糟的结局并接纳它——这样你更可能有机会为更好的结果感到惊喜。

[image]

出庭受审

终有一日，你将不得不登上这个大舞台。理个发，穿套正装，让自己体面些。毋庸置疑，此时对你前景影响最大的将是法官。

你的律师和地区检察官都会设法操纵程序，争取让尽可能有利的法官审理此案。

你将面临法官审判与陪审团审判的选择。陪审团审判中，陪审团判定有罪或无罪，法官则决定量刑（如有）。法官审判中，法官既判定有罪或无罪，也决定量刑。

你不能被强制接受法官审判，如果你要求陪审团审判，则必须予以。

[image]

两种审判方式各有优劣。我虽非法律专家，但可以肯定地说，法官的判决结果比陪审团更可预测——这可能有利也可能不利。

如果该法官声名狼藉，你就绝对不该选择法官审判；

如果该法官声誉良好且检方证据薄弱，法官审判或许更有利。

如果指控内容可能引发随机陪审团同情，陪审团审判更有利；

如果指控内容可能激起陪审团敌意，法官审判则更有利。

法官审判的弊端在于消除了悬案陪审团的可能性。

请听取律师建议，遵循内心直觉，并祈祷自己做出正确选择。

我认为让法庭座无虚席总不会有坏处，但务必确保所有人员都愿对你负责，按你的要求行事或保持沉默。庭审流程通常如下：陪审团遴选→辩护方开庭陈述→检方开庭陈述→检方举证及证人陈述→辩方交叉质询→辩方举证及证人陈述→检方交叉质询→辩方结案陈词→检方结案陈词→陪审团商议→宣判。整个过程的耗时完全取决于案件的复杂程度。变数太多在此不便详述，但可以肯定的是：此刻就是决战时刻。若需出庭作证，请提前进食以免头晕。说话清晰有力，别让检察官扰乱你的心神。

而后一切将结束。要么是一个短途，仅走几步快速跃过围栏便能投入爱人的怀抱；要么，将随法警漫步到后门，穿过走廊，重返那个压迫性司法系统中。如果是第一种，此刻将成永恒的至高体验。你会发誓永不再视万物为理所当然，永不忘却狱友与所有留在狱中的人，并立誓余生每日竭尽所能，让这个世界变得更美好。如果是第二种，你将昂首挺胸，坚韧不拔，像战士一般服刑 —— 因为这既是你的本色，也是你必须承担的使命。你将历经上诉程序，辗转于上诉法院、高等法院乃至最高法院，穷尽一切可能以推翻或减轻判决。或许成功，或许失败。终有一日刑期届满，他们将释放你，那时真正的至高境界将降临。当然，如果你深陷绝境永难脱身，你仍将保持不屈。即便失去所有，你仍会继续抗争，你的灵魂永远自由。

无论如何，青蛙仍会鸣唱，花蕾终将绽放，人们依然彼此相爱，也依然爱着你。人类自筑的这座癌变牢笼正继续摇摇晃晃地走向日益临近

的崩塌 —— 我愿它早日崩塌。我们将持续向这个体系宣战，不断学习与重习如何与彼此、与大地和谐共生——若不如此，我们终将灭亡。倘若众生皆亡，我们终将回归大地，人类的灰烬将在其怀抱中腐化，终有一日，腐殖土中将萌发新的生命。有次绝望至极时，我俯身看见两只大黄蜂在尘土中交配，我意识到这很美好。长远来看，万物终将安好，我真诚地信仰于此。这世上有人服刑的年限比我预想的文明存续时间还要长。当你情绪低落时，不妨想想这个！

记住：你的身体将永远是宏伟生命之网的一部分，植物与动物在此交换氧气与二氧化碳，生与死在此循环往复，腐朽在此重归尘土。你正被绵延不绝的亡灵之躯所环抱，这道无尽的怀抱穿越时空，自创世之初便绵延至今。我们竭尽所能对抗一切虐待与残酷。我们历经千般苦难磨砺，从未屈服。无论发生什么，请记住：我们深爱着你，感谢你所做的一切，你的努力——无论形式如何 —— 都不会白费。

By Crimethinc

[image]
[image]

在敌人的刀刃下 - 寻找反酷刑的无政府主义做法：审讯心理学 S07E05

[image] 关键词	人际安全 信息最小化 关系 安全文化 心理安全 背叛 酷刑
[image] 关联	[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛
[image] 创建时间	2025年3月6日
[image] **Description**	心理安全；行动安全性；反渗透和协作

权力“本身就蕴含着驱使它诉诸屠杀与酷刑的迫切性”。

军事独裁政权必须惯常施以酷刑以确保自身存续。民主政权若尚未惯常施刑，一旦感受到足够威胁便会立即效仿。

酷刑问题关乎所有渴望废除权威制度及其内在力量的人。

- Table of Contents
序言（无痕计划）
跪地之时（巴赫曼）
如何承受酷刑（匿名）
首要挑战自然是肉体痛苦。当酷刑持续不断施

加时，它会变成巨大的精神重压。
还有心理层面的因素。
关于在压力巨大、令人恐慌的条件下开口说话的必要性，有几点需要说明。
如何避免泄露重要信息？
我们珍视的事物都可能沦为条子勒索我们的筹码。
遭受酷刑后令人恐惧。
最后说点个人感受。
酷刑下的抵抗分析（阿什拉夫·德赫加尼）
1. 信念
2. 立场
3. 视角和全局
4. 客观审视现实。
5. 分清敌我
6. 理解和信仰
7. 知己知彼
8. 对自己的信心。
9. 想想同伴。
“对我而言，践行萨穆德就是存在本身”（里亚德）
冷热交织（内森·吉尔伯特·金波）
1
2
3
4
5
为何我们处决了姆潘帕利斯（“1978年6月”）
“但谁配活着？”（阿尔弗雷多·博南诺）
“这是一场冷酷的欢

迎”（安德烈斯·特索帕斯特莱·特克皮莱，约翰·吉布勒）
后记（无痕计划）
我们建议无政府主义者反对酷刑的首要步骤，是在自身处境中评估酷刑的风险与实施方式，包括：
无政府主义者可据此评估制定个体与集体策略，例如：

序言（无痕计划）

酷刑 —— 即为惩罚、审讯或恐吓而蓄意施加的剧痛或折磨 —— 是国家及其盟友在镇压无政府主义者的战争中常用的手段之一。无政府主义者应采取哪些个人与集体策略来防范、抵抗并反击酷刑？

本文集旨在通过分享过去五十年间遭遇酷刑的无政府主义者、共产主义者及其他激进派反抗者的经历与洞见，为解答此问题提供参考。

[image]

酷刑是我们运动面临的最严峻挑战之一。

如何防范酷刑风险？

如何组织行动以确保有同志被捕受刑时，其他同志及运动/行动本身的风险能降至最低？

我们是否应承诺在酷刑下绝不供述？

当遭受最残暴的肉体与精神折磨时如何保持沉默？

如何对待难忍酷刑而选择供述的同志？

如何反击施虐者？

如何帮助酷刑幸存者应对痛苦与创伤？

我们竭力甄选能帮助同志们当下解答这些问题的文本，无需依赖国际法的强制执行或人道主义非政府组织的游说。每篇文本前均附简短导言，介绍作者及原文发表背景。部分文本包含酷刑行为的直白描述。

谨向文本作者及使这些作品得以收录于本集的译者们致以诚挚谢意。

[image]

跪地之时（巴赫曼）

《跪地之时》是伊朗男子巴赫曼所作，其以笔名活动，身兼活动家、马克思主义者与诗人三重身份。

巴赫曼在伊朗监狱遭受了七年残酷的酷刑，后逃亡加拿大。这首诗即写于流亡期间，英文版刊载于2014年论文《诗歌抵抗：见证巴赫曼对抗酷刑与政治暴力的抗争》。

该论文阐释道：

> "巴赫曼自幼梦想赢得奥运奖牌。他坦言，重拾儿时渴望正是其抵抗策略之一。巴赫曼最终得出结论：'若我能保持沉默，若我拥有不泄露任何人名的力量与意志，这便堪比一枚金牌。' [...]
>
> 为揭示巴赫曼的抵抗行为，需详述其遭受酷刑的具体经过。某次刑讯后，尽管他再次拒绝向施刑者提供任

何人名，仍被拖回牢房，双手反铐悬吊八天。解开枷锁时他已无法站立，身陷剧痛。如同每次酷刑体验，巴赫曼不知自己能否挺过下一轮折磨，更无法预知能否再次守住沉默。巴赫曼希望读者明白：下文这首诗绝非隐喻。

当时我
跪倒在地
双脚肿胀
精疲力竭
渴求睡眠
当时他们
气势汹汹
我是那片战场的胜利者
我的武器是沉默
我是冠军
没有观众
没有见证
但我的奖赏远胜金牌
我的奖赏
是朋友们
安然无恙

[image]

如何承受酷刑（匿名）

以下证词来自一位数年前在俄罗斯遭受酷刑的匿名同志。文章基于该同志的亲身经历，描述了承受酷刑的策略。该文于2019年发表于俄罗斯无政府主义网站。

先谈谈我的政治观点。我认为社会组织形式应当造福全体民众，而直接民主是实现这一目标的最佳途径。近来我未参与行动，因为我意识到必须从自身生活方式做起 —— 从人与人之间的关系着手，使其更

直接，学会集体开展共同工作。

[image]

返回：[image]S11关系结构革命-总章节

遭遇酷刑时我猝不及防，从未料到竟有人会出于某种原因对我施以酷刑。当然，唯有亲身经历才能真正体会，但我仍想分享一些反思。我认为以理性方式探讨酷刑具有现实意义。我衷心希望无人陷入类似境地，但事实表明此类事件比想象中更近在咫尺。如果阅读本文者不幸遭遇困境，但愿以下所述能助其以最小代价脱身。不过我并非此领域专家，结论主要基于个人经历 —— 而任何经历都具有个体性，未必适用于其他情境。

需注意的是，酷刑的目的可能各不相同。若不幸遭受酷刑，对你而言最乐观的情况或许是：警方对你个人毫无或几乎毫无证据，他们施刑只是为了获取你与目标人物的关联信息及相关线索（这正是我个人的遭遇）。这些“嫌疑人”本身已受到严重怀疑，警方必然对其进行过跟踪调查并有所发现。或许警方意图调查其所有熟人以期有所斩获，但他们自己也未必清楚具体要找什么，这为我们留下了周旋空间。如果警方怀疑你本人，情况就糟糕得多了 —— 他们会篡改任何他们感兴趣的事实，你将面临更严酷且更持久的施压。若警方已准备将你收监，只需你的供词，情况亦是如此。

[image]

返回 - 镇压手段：[image]对证据的偏见性解读 ；刑侦证据洗白

我将重点阐述遭受酷刑时面临的挑战，以及帮助我部分抵御酷刑的因素。

首要挑战自然是肉体痛苦。当酷刑持续不断施加时，它会变成巨大的精神重压。

人虽能短暂忍受，但终将逐渐说出他们想听的话，做出他们想看到的举动。某一刻你会想发疯，不在乎生死。但这不意味着该立刻放弃。

施刑者也有弱点 —— 他们同样会身心俱疲，即便威胁折磨会持续到他们满意为止。若几小时内未见预期效果，他们可能厌倦折磨你，轮班结束就想睡觉。

你只需耐心熬过这段时日。

还有什么方法？不妨将疼痛与不适视为纯粹的思想——不过是身体细胞发出的神经信号流。当你如此理性认知时，痛苦便不再难以承受。建议在日常遭遇不适时就进行这种心理训练。

还有心理层面的因素。

当你完全受制于他人时，那种感觉极其压抑，如同屠宰场里的牲畜。

努力保留哪怕一丝控制权至关重要 —— 这样才能将现状视为抗争，而非猎食关系。

将头部反复摩擦地板直至疼痛，能让我稍感宽慰 —— 既保留了行动自由的微弱感知，又能掩盖痛楚带来的影响。

割腕自残虽更极端，却也是解脱之道，但切忌过度，况且环境未必允许。

当施虐者以强奸威胁相加时令人毛骨悚然，这迫使我们思考：为了避免泄密，究竟愿意付出何种代价？请记住战友们 —— 此刻此地很可能决定他们的命运，决定他们未来数年的生活。几小时的极度痛苦，是否值得换取他人数年甚至更久的自由？

关于在压力巨大、令人恐慌的条件下开口说话的必要性，有几点需要说明。

当我遭受数小时不间断的酷刑时，几乎无法思考。

同样的问题被反复追问，但你必须开口，且所言必须尽可能保持稳定和逻辑性。

警方在抓捕前很可能已经长期监控你了，追踪你的网络流量、手机基站定位记录、通话及短信内容。因此他们掌握着你生活的诸多细节。

[image]

你必须学会如何解释这些已知信息，且陈述内容需与事实高度吻合 —— 编造既合理又自洽的复杂谎言极其困难。但一旦选定说辞，就必须始终如一。

与其向审讯者提供矛盾的说法，不如装傻。

更理想的做法是提前准备好无懈可击的掩护故事，并让所有相关人员统一口径。

当然并非人人适用，但最可靠的不在场证明莫过于过着平凡生活 —— 工作、学习、培养多元爱好，手机通讯录存满非政治人士的号码，社交媒体主页充斥萌猫照片等。

这种策略有诸多益处：当你承受压力时，无需编造任何内容，只需向警方“如实陈述”，就能证明你本质上是个“普通人”。

[image]

返回 - 相关自卫措施：分身 ；[image]数字技术限制和最佳实践

宜多谈些无关紧要的中性话题，用看似相关却对警方不重要的信息拖延时间，同时避免损害任何人的声誉。若对方执意追问姓名地点等细节，可随意编造，但关键在于避免被构陷为"不明身份者"参与犯罪的唯一嫌疑人。

另一种策略是装疯卖傻说些毫无逻辑的话，不过这需要点表演天赋。

最后谈谈压力应对：根据我的经验，我会努力保持冷静，像旁观者般审视现场，将发生的一切视为梦境或低成本恐怖片拍摄——否则我的大脑恐怕会拒绝感知这些事件。

如何避免泄露重要信息？

首先，从一开始就不要去了解不必要的信息，极其有益。

"知之愈少，眠愈安"——此言不虚。

[image]

返回 - 相关自卫措施：[image]信息最小化原则 ；[image]数字技术限制和最佳实践

大量信息难以保密，在没有实际必要时试图获取敏感信息亦非明智之举。

[image]

重要信息应仅通过加密设备在相对安全的场所访问，

所有关键密码都应存储在密码管理器中 —— 你甚至无需查看它们。

通信可采用Jabber配合OTR加密，

或在安全服务器上使用PGP加密邮件。

但你需要提前准备好使用加密的合理解释。因为统治者认为加密是“有所隐瞒”的行为。

遭受酷刑时，你完全可以隐瞒部分信息。例如我坚持原则：不透露无

关姓名，不诋毁任何人——因为这些人很可能同样遭受酷刑。由于警方并不知晓我实际认识这些人士，他们不久后便放弃了逼供。

我们珍视的事物都可能沦为条子勒索我们的筹码。

失去所爱之人 —— 挚友、亲人、荣誉、自由乃至生命 —— 皆令人痛彻心扉。但须谨记：那些以剥夺上述任何事物相威胁者，即便你屈服，他们照样能轻易实现目的。

若你已完全受制于人，便再也无法守护任何人或任何事物。

最荒谬的莫过于相信将你逼入绝境之人的承诺。更别以为生命本身具有非凡价值 —— 许多人会为达成目的甘愿牺牲它。

警察或许会虚张声势，声称你已被举报，否认也无济于事云云。诚然，任何工作中都需要信任合作对象，但若对亲密伙伴存疑却仍携手重要事业，实属愚蠢行为！建立足够的信任与默契往往需要漫长时光，有时甚至需经年累月。对于完全信任之人，除非遭受酷刑逼供，否则绝不能认定其背叛。

如果参与由互不相识者组成的大型团体活动，则必须预设部分成员会主动或被动向警方泄密，因此必须构建团体运作机制以最大限度降低此类风险。

理解施虐者的心理并向其传递符合其价值观的信息也很有帮助，试图寻找共同点。例如，诉诸上帝的报应，认同"乌克兰的那些班德拉分子确实太过分了"，并以"我不需要这些革命，我有其他事情要操心 —— 盖房子、买车"等理由反驳指控。

遭受酷刑后令人恐惧。

当然，我绝不会在不看内容的情况下签字，但我的意志显然已被削弱，非常害怕酷刑会重演。获释后，这种恐惧持续了相当长一段时

间，我害怕独处，更不敢上街。

最初阶段，值得信赖的人陪伴在侧至关重要，他们能协助解决住所及其他所需事宜。

同时应备有律师联系方式、媒体联络渠道、有效护照签证及备用通讯设备。

[image]

我认为事件发生后应立即记录伤情并公开案件。

创伤中心会即时向警方通报信息，这可能无益于案件处理，因此最好直接找私人法医鉴定。

媒体曝光虽非防止酷刑重演的万全之策，但警方极可能不愿再次引发关注，这有助于让他们不再骚扰你 —— 而无人关心的受害者则可能遭受无限期折磨。不过，此后继续留在俄罗斯生活仍属危险之举。

最后说点个人感受。

酷刑这种事的影响力极其强大。我不会说在此之前对人性怀有幻想，也不会说经历之后不再爱人——或许正是这些特质让我相对容易承受酷刑。

然而我内心确实发生了变化，或许是对自身痛苦与他人痛苦变得更为敏感，但这种感受也变得更自然了。从内在而言，很难判断这些变化究竟是有益还是有害。

简言之，酷刑不过是掌控者手中的又一工具。无需对此惊惶失措，但必须认清其运作机制并思考应对之道。愿酷刑的威胁不会阻碍你们追求个人与集体的梦想，更愿你们无人承受酷刑之苦。

若有人不幸遭遇，愿你们坚韧不拔，坚信自身力量！

[image]

酷刑下的抵抗分析（阿什拉夫·德赫加尼）

《酷刑下的抵抗分析》由阿什拉夫·德赫加尼于1970年代初撰写，作为其狱中回忆录《伊朗的酷刑与抵抗》中的一个章节，该书于1976年被译成英文出版。

阿什拉夫·德赫加尼（1949年生）是伊朗共产主义武装分子。1971年她加入地下游击组织"伊朗人民敢死游击队"（OIPFG），同年被捕入狱。

在狱中她屡遭酷刑折磨，从始至终抵抗残暴对待，未向施刑者透露任何敏感情报。

1973年越狱后重返OIPFG组织。

1979年伊朗革命推翻伊朗帝国政权后，当部分同志放弃游击战争时，阿什拉夫·德赫加尼组建新组织IPFG 继续对新政府进行武装斗争。据称她后来移居欧洲，现下落不明。

[image] https://z-library.sk/book/18326848/a79cc3/torture-and-resistance-in-iran.html

---

能够帮助同志抵御酷刑的因素可概括如下：

1. 信念

对革命道路正义性的坚定信念：这种信念必须坚如磐石、不可动摇，

即便在极端情况下所有同志都背弃斗争时，它也不会动摇或减损。

如果没有对我们所奋斗的理想的坚定信念，就不可能抵抗酷刑以及敌人的一切诡计。

2. 立场

对敌人的憎恨与对战友的热爱：这些情感如此强烈，以至于成为战士整个生命不可分割的一部分。

对我而言，想到自己竟可能因泄露姓名而让另一位战友承受我正在经历的酷刑，简直难以想象。

怀着对战友的深情与对敌人的无尽仇恨，我怎能成为将战友送入刑讯室的帮凶？

目睹他们受刑的痛苦，远比我自己承受的折磨更令人煎熬。如果我心存任何其他念头，便是对所为事业的彻底背叛。

为逃避酷刑而将战友出卖给刽子手，意味着要承受终生的精神折磨 —— 这是我绝不接受的。况且，向可恨的敌人投降，于我而言等同于憎恨人民。

[image]

敌人以为我们举起武器是为了谋取高位。而我深知，我战斗是为了将人民从剥削者的魔爪中解放出来。

向敌人投降意味着我背弃了人民，放任剥削继续肆虐；

意味着我参与了整个骇人的剥削勾当。

毕生淬炼使我憎恶一切剥削者；想到自己竟可能顺从其意，便觉恶心

反胃。

难道此刻我竟能忘却身陷枷锁的同胞？那可是我始终怀着深情厚爱的人民。

敌人的罪行如此真实昭然，令我难以视其为人类。故投降念头从未萌生。

3. 视角和全局

从辩证法角度看，无论是短期还是长期实现，抵抗与革命胜利之间都存在着必然联系。

短期而言，我们的抵抗或许能挽救同志免遭敌方俘虏，或阻止对组织的袭击。但更重要的是，这种抵抗精神 —— 这种拒绝投降的意志 —— 正是迈向革命最终胜利的步伐。

若孤立审视这"一步"，它或许微不足道，但切莫忘记无数同志正以同样方式进行着抵抗。

试想所有抵抗的累积效应，便会明白：退缩一步、放弃抵抗即是背叛革命。

因此，以正确视角审视全局，将增强我们抵御酷刑与敌方诡计的抵抗力。

4. 客观审视现实。

就酷刑而言，引发恐惧、丧失斗志和抵抗精神的根源，与其肉体伤害无关，主要在于人们对其形成的普遍主观认知。这种认知更因伊朗情报安全局（SAVAK）关于酷刑的蓄意宣传而被放大。

但若客观审视，酷刑这桩龌龊行径便会失去实质意义。

归根结底，酷刑之下最严重的不过是死亡，这对革命战士而言并非难题。心理折磨确实会影响那些无法保持客观的人。例如当他们剥光我的衣服时，我这样分析：赤裸的腿与赤裸的手并无区别，因此拒绝为此动摇；又如当手枪枪口抵住太阳穴恐吓时，其最终的物理效应不过是颗致命子弹 —— 既然我为事业赴死毫无畏惧，这显然毫无意义。

因此，客观分析事物至关重要，唯有如此才能以更强大的力量直面敌人。

5. 分清敌我

对敌人必须永远地绝对地不信任。

敌人对俘虏所作所为的动机只有一个：迫使战士吐露机密，从而削弱革命运动。仁慈、酷刑、威胁、辱骂、各种背叛者抛弃理想的故事，皆为此目的而设。

因此，我们必须时刻保持警惕面对敌人，对其行为保持怀疑 ——无论看似重要还是微不足道。

忘记这一点将致命。

[image]

拒绝接受敌人的善意举动至关重要。

孤独、持续的折磨与精神消耗，正是滋生妥协的温床。

敌人的善意举动背后暗藏险恶。稍加抵抗便能揭穿其真实意图，同时也能坚定战士的意志。

6. 理解和信仰

对"自由"与"囚禁"等词汇的正确而哲学性的理解：在酷刑与锁链之下，我始终感到自由 —— 这确是真实的。保守主义的念头从未阻碍我用自己选择的语言表达对敌人的憎恨。

我已为信仰事业奉献一切，此刻唯余信念可守。

我深知施刑者完全依赖于卑微可耻的日常琐事，这份认知成为我的力量源泉。

我坚信作为人民的战士，审判者应当是我，主宰者应当是我。倘若屈服于他们，便等于彻底暴露自己的无能。我深信我的信念与追求远非他们所能理解。

这种身陷囹圄却无所不包的自由感，反而增强了我的抵抗力量。

7. 知己知彼

对敌人手段的预先了解：必须研究其他同志应对敌人诡计的经验，以便予以化解。

例如敌人试图找出某人的弱点并加以攻击，我们只需拒绝暴露弱点即可。

又如，敌人精心编排一组常见且无用的数据，企图向战士施压，使其相信敌人无所不知。如果战士事先知晓此敌方伎俩，便能识破其意图，保持镇定自若。

8. 对自己的信心。

对人类意志力的坚定信念：只要我们有意识地强化这种信念，敌人那些关于催眠术、注射药物、强行灌服某种据称能在囚犯睡梦中迫使其吐露秘密的药剂的花言巧语，便会失效。

这种信念在抵御痛苦方面尤为有效。

因此，在遭受酷刑时，我曾长时间感觉不到疼痛。当酷刑持续延长时，我才迫切渴望结束。

然而纵有此念，我从未感到意志动摇，因我深知痛苦终有尽头 ——死亡。在死亡降临之前，我决心挺直脊梁。因此，是否招供的问题从未构成实质困扰。

需在此说明：在日常生活中，贝赫鲁兹同志与我始终致力于强化自身的信念力量。

9. 想想同伴。

想到其他战士的顽强抵抗和他们勇敢对抗敌人的姿态。

世界运动史中处处可见战士们史诗般的抵抗；伊朗人民的斗争史亦是如此，尤其近些年更是如此。

这可以成为所有真正战士的力量源泉。

习惯自欺欺人、未能以革命诚实面对自身过失甚至欺骗自己的人，最可能沦为叛徒 —— 因为谎言正是背叛的开端。

[image] 阿什拉夫·德赫加尼于1970年代的影像 [image]

“对我而言，践行萨穆德就是存在本身”（里亚德）

以下无题证词由巴勒斯坦人里亚德分享，并收录于约旦河西岸伯利恒大学学者莉娜·梅里2014年论文《萨穆德：殖民监狱中的巴勒斯坦抗争哲学》英文版。

自殖民计划启动之初，以色列国便惯常对被俘巴勒斯坦人实施酷刑。

20世纪60年代末，"萨穆德"（源于阿拉伯语"ṣumūd"，意为"坚韧不拔"）作为文化价值与抵抗殖民占领的策略，在巴勒斯坦民众中应运而生。

此后数十年间，正如本证词所示，巴勒斯坦武装分子将萨穆德精神运用于抗击酷刑。

尽管萨穆德是巴勒斯坦民族特有的精神，但我们相信其核心的归属感可在其他社群中发掘或培育。

无政府主义者尤其能从中汲取灵感， 发展出独特的文化政治价值体系，助力同志们抵抗国家暴力。

1991年，为躲避逮捕隐秘六个月后，我前往探望父母。

占领军前来逮捕我，我在逃跑时受伤。

照例，车上又开始了殴打和辱骂。当时我正研读《抗争哲学》等著作，思绪飘向萨穆德精神。

在审讯中心，我不断在"沙巴赫"与审讯室之间穿梭（沙巴赫是一种酷刑手段，有点类似文革中使用过的酷刑“喷气式”，即通过将目标人以极为痛苦的姿势捆绑起来以令其妥协）。

他们施展各种手段 —— 剥夺饮食睡眠、关进储物柜、塞进冰箱、强

力摇晃 …… 他们将我父亲带到审讯室，并威胁要带我母亲来。

十二名审讯员轮番审问我。[…] 每次审讯中，我都在构思践行坚韧的策略。

我所说的审讯中的坚韧，是指集体精神、对巴勒斯坦正义事业的信念、真诚与忠诚、归属感、自信心，以及在漫长岁月里滋养自我的力量。

在漫长的审讯与酷刑中，我将坚韧视为守护母亲与他人母亲的盾牌。我时刻铭记烈士、囚徒与坚守中的巴勒斯坦同胞。我思念烈士易卜拉欣·拉伊，不断吟唱萨布琳的歌曲（阿拉伯语“耐心”、“忍耐”）。我深爱着一位姑娘，相信唯有践行坚守才能配得上她的爱。对我而言，践行坚守即是存在。

[image]

冷热交织（内森·吉尔伯特·金波）

下文节选自《颠覆人生：马科斯统治时期的家族回忆录》中"冷热交织"一章，该书由金波家族成员共同撰写，记录了他们从1960年代至1990年代在菲律宾反抗马科斯独裁统治的历程。

本章由内森·吉尔伯特·金波执笔，详述了他1976年遭军方逮捕和遭受酷刑的经历。

内森时任菲律宾共产党（CPP）成员，该地下革命组织致力于对抗独裁统治。被捕前一个月，内森刚从菲律宾首都马尼拉迁至宿务市，奉CPP之命开展"宣传与文化工作"。他在朗贡居民区的[image]藏匿点或安全屋 与CPP同志拉尼、厄尼、伊芙琳共同生活。

我们认为本文是向施虐者提供虚假、无用、误导性或不完整信息做法的典型案例，既揭示其潜在风险，也展现可能带来的益处。需注意的是，尽管文中描述的酷刑手段极其残暴，内森在2019年接受鸭嘴兽联

盟社团采访时坦言，自己遭受的折磨"与其他活动家的遭遇相比根本不算什么"。

1

[...]

“跟我们走！”其中一人拽住我的手臂用力一扭，随即给我戴上手铐。那群人把我推搡着往门口挤去。[...]

他们戴着手铐把我带到户外，穿过大学校园来到繁忙的街道。光天化日之下，绑匪们若无其事地招手拦下出租车。我被塞进后座，蒙着眼睛夹在两名男子中间，还被命令低头低头，把脑袋顶在膝盖上。

摘下眼罩时，我发现自己被铐在看似普通教室的课桌椅上 —— 讲台椅、课桌椅，前墙挂着黑板。唯一显得格格不入的是堆在角落的木板。除绑匪外，几名便衣人员进进出出。他们搜查了我的身体。身上除衣物外仅有零用钱，连钱包和身份证件都没有。他们采集了我的[image]指纹 ，让我填写表格。

我填写了虚假信息。姓名？莱昂纳多·布恩苏塞索。[...] 住址？马尼拉圣米格尔区圣贝达小区第二街542号。多年前我们家住在第二街538号，542号根本不存在。

填写表格时，我构思着审讯时的说辞。

我的掩护故事是参与教会研究项目，调查维萨亚斯地区学生的宗教与社会生活。刚抵达宿务，不久就要离开。是的，我会告诉他们我9月20日抵达，而非9月8日。这样若需交代在宿务的行踪，只需编造过去三周的故事。如同上次被捕时那样，我会暂时隐瞒真实身份以争取时间。同时决定不透露自己曾是政治犯的身份。

为缓解紧张情绪并拖延审讯，我应允与两名男子下棋。近一小时后午

餐送达 —— 米饭配肉菜的正经饭食。尽管心绪不宁，我仍细细品味着米饭，毕竟过去一个月我和同志们为省钱只吃玉米粉。

随后进入审讯环节。房间里的男人们如连珠炮般向我发问。

“你真的叫这个名字 —— 莱昂纳多·布恩苏塞索？”

“是的。”

“是的，先生。”

“是的，先生。”

“简称莱奥？”

“是的……先生。”

“你住哪里？”

“圣贝达小区第二街542号。我已经写在您给我的表格上了……先生。”

“ 但这是马尼拉的地址。你在宿务的住址呢？”

“我不住在这里。只是来做几周研究。”

“研究啊？你现在住哪儿？”

偏偏忘了准备宿务的地址。一时想不出——去过的都是同伴或盟友的家。“啊——天景酒店，”我终于脱口而出。

“天景酒店？你住得起天景酒店？房间号是多少？”

“记不清了，先生。”

“你真住在那儿？这很容易查证。登记时用的什么名字？”

“莱昂纳多·布恩苏塞索。”

“联系天景酒店，”那位看似负责的男子指挥年轻探员。

完蛋了，我暗自哀叹。这次再也无法搪塞过去。

几分钟后探员返回。天景酒店没有登记过莱昂纳多·布恩苏塞索。我无法描述天景酒店大堂和房间的样貌来佐证我的说法，毕竟我从未踏进过这家酒店。

特工们逼问我在宿务的真实住址。我坚持说天景酒店，要么就保持沉默 —— 毕竟实在想不出其他地址。他们继续追问：何时以及如何加入运动和菲律宾共产党的？谁招募了我？我的同事是谁？

编造我在马尼拉的政治活动倒不难。只需提及戒严令前在 KM-Ateneo 的经历，坚称后来转学至UP便销声匿迹。我否认入过党，被要求提供人名时，要么杜撰，要么提及已故的或曾被捕的同志。

真正让我陷入困境的是宿务 —— 这个陌生的地方。何时抵达？去过哪些场所？执行什么任务？见过哪些人？当我拒绝回答时，审讯者扬言要殴打我。他们对不满意的回答反复追问，或不断重提旧问。

被揭穿谎言后，我竟 不敢 鼓起勇气质问他们依据何种罪名拘押我。

审讯者拒绝相信我在宿务主要是在公共图书馆和学校图书馆做研究的说辞，也驳斥了我声称9月20日才抵达宿务的说法。他们显得越来越愤怒。

当他们发现我拒绝配合且审讯毫无进展时，他们改变了策略。

2

冷热交替（就是中文所言之“红白脸”）。卡萨马审讯术语中常有这两个词出现，用来描述战术性审讯。这意味着数小时的严酷殴打后，会出现短暂间歇。一位看似同情、言语温和的军官会驱散施虐者，单独与你交谈，劝你坦白以保全性命。如果你坚持沉默，整个过程便会循环往复，直至审讯者达成目的或厌倦这场游戏。

热。

他们摘下我的眼镜，再次蒙住我的双眼。左手仍被铐在椅子上，约十二名男子开始对我施暴。砰！一块木板砸中头部，我痛呼出声。

"你在宿务住哪儿？哪儿？" 沙哑嗓音厉声喝问。

砰！后背又挨一击。我惊恐地意识到那些摆放错位的木板用途何在。

"你住哪儿？"

他们拳脚并用，猛击我的面部，用空手道劈掌砍向我的肩膀，踢打我的双腿。

"什么时候来的？"

"来这儿执行什么任务？"

“你是中共党员吗？”

“住哪儿？”

那是我这辈子头一回挨揍。每次板子我都痛得嚎叫。我拼命挣扎，但左手仍被铐在椅子上动弹不得。当我挥舞右手时，手表砸到某人身上。他们一把扯下表。我哀求道：“求求你们停手。可怜可怜我吧！我贫血啊。”这话并非实情，只是想让他们停手。体重不足百磅的我，贫血倒也说得通。

见我仍不屈服，他们剥光我的衣服，将一根通电的线 —— 可能是电话线 —— 抵住我的生殖器和大腿。我尖叫起来。他们继续殴打我。当我再次喊叫时，他们塞了块布进我嘴里。

他们继续施暴。"还不说？"其中一人问。更多拳脚。同样的问题。更多……

最终我点头了。他们解开蒙眼布，又扯掉堵住我嘴巴的布 —— 我才看清那竟是我的内裤。我抽泣着告诉他们身份：曾在伊皮尔被拘留，兄弟都是前在押人员，妹妹正在服刑。

我解释自己申请调往宿务工作，是因为在马尼拉已被军方盯上。我承认是菲律宾共产党候补党员。

当被问及入党推荐人时，我提到了比尔·贝格，却未提及他已遇害。

我努力在抽泣间尽可能长时间地继续供述。我提供的信息对审讯者尚属新知，但金波地区逮捕拘留行动的全部细节早已载入军方档案。实际上我并未泄露任何敏感战术情报。然而审讯者很快识破我的策略，再度逼问宿务住址。

冷。

这次他们没有殴打我，而是改用花言巧语。“你为什么不配合我们？”一位看起来像父亲的探员说着，把手搭在我的肩上。

“看看你现在的样子。我们不想这样对待你。”

他们解开了手铐，允许我穿上衣服。他们把我的眼镜和手表还给我。

更多“建议”的话语。随后他们端来点心 —— 饼干和可乐。待我吃完，桌上突然出现纸笔，命令我详述抵达宿务后的行踪：列出接触人员的姓名和特征，标注所有去过的地点 —— 否则后果自负。

我明白这些人除非得到我在宿务的住址，否则不会罢休。

但透露拉邦贡的住所绝无可能 —— 若我这么做，拉妮、厄尼、伊芙琳和其他同志必遭捕杀。

我能提供什么地址？要是能找到明显与政治无关的人家，或是废弃的邮局，或是空置房屋就好了。

可我脑中一片空白。突然想到：我的被捕必然导致拉邦贡的住所被弃用。现在不能透露地址 —— 必须给同志们足够时间撤离。

同志们的惯例是：地下安全屋必须在任何曾在此处的人被捕后24小时内弃用。

战友们直到傍晚我未归时才会意识到我已被捕。为确保他们有充足逃离时间，我必须忍受酷刑并拖延至次日晚间。我能撑那么久吗？

热。

那些人又回来了。我面前的纸上什么也没写。他们暴跳如雷。把我转到更小的房间。殴打以更猛烈的强度继续。我被迫长时间站立，手铐被解开，但仍蒙着眼睛，且被剥得一丝不挂。除了对我身体猛击和掌掴，他们还把我的头撞向水泥墙，用枪托猛击我的手背。

多次遭受重击后，我踉跄倒地，痛苦地呻吟。

我放弃了关于天景酒店的杜撰故事，却想不出其他说法。

除了逼问住址，施刑者不断追问我何时抵达宿务。他们坚称我谎报了入境日期。

我坚持说是9月20日。最后他们亮出一张照片，清晰拍下了我和另外三名卡萨马成员。我们正从一条小路走向看似主干道的街道，照片显然是从马路对面二楼拍摄的。

没错，我认出了地点 —— 卡巴胡格！那正是我初次与拉尼会面的地点。这个会合点显然已被军方掌握多时。我努力回想那次会面的具体时间。照片拍摄日期应是9月18日，比我声称抵达宿务的日期早了两天。难怪施刑者们拒绝相信我9月20日抵达的说法。

承认9月20日的说法同样站不住脚后，我坦白了真实抵达日期 —— 9月8日，甚至提供了乘船名称"宿务市号"及当时使用的假名。

但我强调自己是独自前来的，抵达后才遇见宿务的同志，此后他们便一直照料我。

"码头接你的人是谁？" 沙哑嗓音问道。他似乎是主要审讯者。

"卡永，照片里那个人。" 虽然罗德也在照片里，我却指向了记不清名字的另一人。心念一转：打不过就糊弄过去。

“照片里其他是谁？”

“不清楚，长官。我只在那次聚会见过他们一次。”

我编造的新说辞是：自己被辗转安置在不同住所，外出时总有同伴随行，独自一人根本无法辨认去过的房子。

审讯者逼我描述所有提及的住所及屋内遇见的人。

为验证我是否杜撰人物，他们每隔十分钟或二十分钟就让我重新描述某人。总体而言我保持了前后一致 —— 诀窍是选个真实人物，比如马尼拉某个不涉政的朋友，稍改其名后进行描述。

"你见过托尼·T吗？"

"不记得见过这个名字的人。"

"他化名德里奥。" 他们递来一张照片。尽管画面模糊，我确信这就是在宿务为我安排任务的人 —— 两年前在洛约拉高地见过面的同一个人。

"没有，先生。" 我面不改色地回答。

第二次审讯结束时，审讯者仍未能逼出我在宿务的住址。"总有办法弄到的，"其中一人发誓道，"夜还长着呢。"

3

他们给我上了晚饭。担心再挨打会消化不良呕吐，我只吃了几口。但喝了不少 —— 那场折磨让我汗流浃背。

晚饭后不久，第三轮审讯开始。那些人浑身酒气，说话粗鲁。

我的不安加剧了。他们还能控制住自己吗？

即便经历六小时的拷问折磨，我仍未向审讯者透露任何真正有战术价值的情报。我察觉他们心知肚明，更因被我戏弄而愤懑。

尽管如此，我仍复述了第二轮审讯时编造的故事。

再次被蒙住双眼、剥得精光后，殴打重启。

由于他们再也找不到故事中的矛盾或重大漏洞，我坚持着新编的版本。我的掩护故事站得住脚 —— 除了宿务的地址。很快，施暴者将审讯焦点完全集中在此处。这是他们唯一能加以战术利用的线索。我察觉到他们此刻正与时间赛跑。他们深知若不能立刻逼出地址，藏身于此的其他同志便能逃脱。

"砰！砰！" 部分拳脚落在了我的下肋骨上。这次殴打比第二轮更猛烈更持久。

我多次倒地，但每次都被拽起来继续遭受拳打脚踢和空手道劈掌。最痛的是他们将我的头撞向墙壁，我以为自己会昏过去。尽管我已精疲力竭，他们仍持续施暴数小时不作停歇。

"要不要像对付你战友那样给你注射'吐真剂'？" 沙哑嗓音威胁道，"它能逼你吐实话。我们其实不愿动用这招，毕竟会造成永久性心理创伤，甚至可能让你疯掉。"

我从其他囚犯口中听说过这种药剂。它并非强迫人说真话，只是让人变得喋喋不休，更容易说出那些本该守口如瓶的事。有时确实会造成永久性心理创伤。

"不，求求你们。不，先生。"

"那你最好告诉我们藏身之处。"

殴打仍在继续。他们为何不停止？我感觉自己已濒临崩溃边缘，再也承受不住这些打击。明晚似乎遥不可及，宛如永恒。

这时一个念头闪过脑海：假装他们已攻垮我，编造一个宿务地址？这

样行得通吗？他们不会要求我描述房子的内外细节吧？尽管如此，我还是决定一试。我已走投无路。

"雅可沙莱姆148号！" 他们继续殴打时我喊道。据我所知，雅可沙莱姆是条长街，以住宅区为主但也有商业设施。我祈祷148号是民宅而非商铺，这样故事才显得可信。

"住手！住手！" 沙哑嗓音喝止。殴打戛然而止。那人凑近我问道："你说什么？"

"雅科萨勒姆1-4-8号，先生。" 我嚎啕大哭，彻底崩溃。他们扯下蒙眼布，泪水如泉涌出。多么戏剧性！小学和中学时我参演过许多话剧，甚至获得过几次表演奖，但校园剧场与此刻上演的剧本相比根本不值一提。这才是我人生中最精彩的表演。

奏效了！以为终于折服了我，那些人懒得询问148 号的具体描述，反而用他们惯用的虚伪方式安慰道："别哭了。你的折磨结束了，可以休息了。看吧，若早些配合我们，就不会受这么多苦。"

我讨了水喝，他们给了我一杯水和一瓶装满水的家庭装可乐瓶。我一口气喝光整瓶水。浑身黏腻难耐，我请求洗漱。他们"慷慨"地允许我淋浴。我用手帕擦干身体，反复拧出水分。当他们把我铐在小房间的床上时，已近凌晨四点。

想到这些人稍后发现我报了假地址会对我做什么，我不免心生不安。辗转良久，我才终于睡去。

4

那天和次日都没有关于148号的消息。他们不太可能突袭了那里 ——要是突袭了，我怕是要再当一次出气筒。最可能的情况是，他们已将那里置于监视之下。

我仔细检查了他们施加的虐待痕迹：头顶几处肿块，嘴唇与脸颊麻木，左腕附近淤青肿胀，全身多处瘀伤疼痛。所幸没有骨折，生殖器未留痕迹，没有永久性毁容。我的脑袋还完好无损。

我推断施虐者必定刻意避免造成永久性损伤或留下明显伤痕。以我瘦弱的体格，胸口若遭重击本应断裂数根肋骨。后来其中一人竟声称他们的拳脚都"分寸得当"。

[...]

5

哈士奇嗓音的人冲进房间，脸色涨得通红。"你骗了我们！" 他怒吼道，"你给的地址是假的！"

"什——什么意思？" 我装作一头雾水。

"你报的地址 —— 雅科萨勒姆148号 —— 那是家诊所，牙科诊所。根本没人住！现在最好老实交代真实地址，否则我们非把你打得半死不可！”

他不等我回答，狠狠扇了我一记耳光，接着又朝我腹部猛捶一拳。其他男人涌进来加入殴打。他们开始粗心大意 —— 竟忘了给我蒙眼。

“拉邦贡，” 我平静地说，“是拉邦贡的一栋房子。”

他们停下了殴打。"门牌号？" 其中一人怀疑地问，同时向我展示紧握的拳头。

"没有门牌号。那里的房子都不编号。你们坐吉普尼的话，在圣伊西德罗小教堂拐角处下车。过桥后第六栋房子，右侧，紧挨着一家小杂货店。”

他们让我详细描述屋子内外。我照做了。他们似乎终于相信我说实话了。

几分钟的盘问和听我描述后，他们匆匆离开房间。看起来他们当晚就要发动突袭。

不过他们肯定会一无所获。我瞥了眼手表暗自盘算：被捕至今已逾78小时。随即又忧心忡忡——万一卡萨马违反安保规定，仍未撤离那栋房子呢？

当晚杳无音讯。次日亦无动静。但无消息或许就是好消息 —— 没有新的逮捕行动。

被捕第五天，他们放进一个秃顶中年男子，提着医生包挂着听诊器。他草草检查了我。酷刑留下的痕迹虽已消退却仍清晰可见，他对此只字未提。他问我是否贫血。或许我的贫血说辞终究奏效了，让那些人收敛了拳脚的力度。我点头。他检查了我的指甲，又掀开我的眼皮。"没有贫血，"他断言。医生离开后，我再未见过任何医疗证明。我猜审讯者只是想确认他们的拳头没在我身上留下永久印记。

审讯者们打出一份供词，声称我参与颠覆活动。他们逼我读完并签字。这份供词荒谬地自相矛盾，包含我杜撰的内容，包括雅科萨莱姆和拉邦贡的故事。

[…] 我签了字。日后要推翻一切都轻而易举。[…]

[image] 内森·吉尔伯特·金波，2009年 [image]

为何我们处决了姆潘帕利斯（“**1978年6月**”）

本文节选自希腊革命组织"1978年6月"于1979年刺杀彼得罗斯·姆潘帕

利斯后发布的公报。

彼得罗斯·姆潘帕利斯曾在希腊1967至1974年军事独裁统治时期担任酷刑施虐者及警察。独裁政权垮台后，因其对政治犯实施酷刑，姆潘帕利斯被判处18个月监禁。

"1978年6月"组织很可能隶属于"11月17日革命组织"——一个希腊城市游击组织。

我们分享此文，作为革命者通过物理消灭施虐者来反抗国家酷刑的众多案例之一。

截至今日，可憎的酷刑施虐者、警察佩特罗斯·姆潘帕利斯已不复存在。他被一队战士处决。其为人行径众所周知。在军政府统治时期，他的恶行与恶名早已超越希腊国界。

作为镇压力量的首脑之一，他执掌着阿斯法莱亚的迫害机器。他以极端残暴的手段打击反抗军政府及其背后的体制的战士。

他主导着阿斯法莱亚的恐怖统治，对成千上万民众实施骇人听闻的酷刑。他摧毁了数百名战士的身心健康乃至生命，不仅如此，凡是因任何缘由落入阿斯法莱亚之手者皆难逃厄运。他一手扶植数百名告密者（线人）成为精英酷刑执行者，其中许多人至今仍在继续作恶，正日益成为资本家统治集团国家机器的核心支柱。

[...]

因此，我们 —— 作为我国人民革命运动力量中的一支战斗队伍 —— 决定处决佩特罗斯·姆潘帕利斯：

因其身为阿斯法利亚臭名昭著的酷刑施虐者与警察，必须为无数罪行付出代价；

因为他即便在结束酷刑行径后，仍持续充当政权针对无产阶级的"非正式"镇压与恐怖机器的重要工具及自觉参与者；

因为通过他及其行径，资本主义权力体系的暴力与压迫实现了特定的"代表功能"。

这种"代表功能"是维系剥削与压迫的具体而持续的实践，绝非抽象的"制度"。我们将以具体而持久的斗争对抗这种暴力与滥权行径，而非模糊的宣言与抗议 —— 事实证明，后者不仅毫无助益，更会分散注意力、安抚人心，削弱一切斗争的意愿与决心。

[…]

发展人民暴力革命，对抗政权恐怖统治与资本家的剥削。以一切手段打击警察及其支持机构。唯有通过人民革命斗争才能推翻统治 —— 斗争仍在继续。

[image]

“但谁配活着？”（阿尔弗雷多·博南诺）

以下文字摘自阿尔弗雷多·博南诺2013年出版的意大利语著作《不速之客》。

阿尔弗雷多·博南诺（1937–2023）是意大利无政府主义者。作为起义无政府主义的倡导者，他毕生通过文字与行动践行理想，曾多次遭监禁酷刑。

本书成书于2010年，当时他因涉嫌银行抢劫案在希腊服刑期间完成创作。在《不速之客》中，阿尔弗雷多详述了1970年代其亲身参与的全球各地暗杀行动：在希腊对抗军事独裁政权，在巴勒斯坦反抗以色列殖民统治，在北爱尔兰打击英国殖民势力 —— 目标均锁定酷刑施虐

者、告密者、叛徒及其他国家镇压机器的代理人。

贯穿全书的"不速之客"意象，象征着毫无预兆降临的死亡 —— 这是阿尔弗雷多及其战友在执行暗杀任务时所扮演的角色。

在回忆北爱尔兰行动的这段文字中，阿尔弗雷多对过往行为产生了质疑，并尝试对杀害酷刑施虐者等国家"怪物"的行为进行伦理审视。

我常发现意外的访客就在身旁。在工作中遇见它，永远无法习惯。碾碎、根除、摧毁生命 —— 这便是它的存在方式，一种无人渴求的意外存在，如同令人厌恶却又不得不为之的卑劣正义。

参与其中需要充分准备，并非技术层面 —— 那反而是最不需担忧的 —— 而是个人层面的、私密的、道德层面的准备。它的存在既令人不安又充满魅力。片刻之前还是鲜活生灵的存在，饱含生命力，能憎恨、能爱慕、能期待、能繁衍，未来本可赋予他无限可能 —— 却因邂逅这位不速之客，骤然丧失一切能力。他横卧地面，被碾得粉碎，如同断线的木偶，一块旧布，一团静止的血肉，数日后便将开始腐烂。这股善恶交织的爆发力去了何方？它化作烟消云散，被不速之客攫走带走。

[...]

少了一个怪物。多少酷刑得以避免？类似我亲身承受的，以及那些素未谋面的他人所受的。这等怪物不配活着。值得深思的判决。

但谁配活着？行为端正者。可何为行为端正？遵守规则？免于酷刑。数百年监禁、合法处决与种种刑罚。这算守善吗？手持法官签字的纸条杀人者，真比奉命施刑杀人者责任更轻？得了吧，认真点。

若真认真起来，活人所剩无几。

界限何在？谁来划定界限？界限清晰吗？抑或随意勾勒，稍有偏差，

此人便在界内，彼人便在界外？

当探讨其极端后果时，这便成了棘手的议题。谁来裁决？谁来执行？**[...]** 这种彻底的割裂 **[...]** 不仅消除了人类的暴虐 —— 唯有人类能如此暴虐 —— 更是扼杀了所有批判性思考。所有问题都悬而未决。

即便在我们组织内部，也有人坚信自身行为的正当性，有人心存疑虑。

[...]某些人类、某些任务、某些国家机构，或是赏金猎人与雇佣杀手所展现的暴虐，难道不该不惜代价连根铲除吗？

不惜代价？当然，代价评估始终不可或缺。若以杀戮怪物之手段行杀戮之实，无异于以暴制暴，甚至加倍屠戮。

故需明辨是非。在地下斗争的炽热中，这种明辨是否难以企及？在外国军队占领的国度行动时，是否难以实现？或许吧。

抑或存在未曾考虑的替代方案？更注重情报分析？更精准谨慎地选择目标？我们是否时常冒着攻击最软目标的风险？某些行动是否只是为了在胸前再添一道象征性的勋章？我不得而知。

我并非断言事实确是如此，而是坦言自己多年心存的疑虑。

作为秘密作战单位，我们必须展现存在迹象。行动、持续核查比对、实施任务、召唤意外之客。秘密作战单位还能做什么？咬指甲吗？但究竟是谁赋予了意外之客那份至高无上的权力 —— 那份我们历经艰辛才托付给他的权力？

绝非都柏林运动组织提供的信息—— 那些情报几乎仅限于背景资料、地点简述和零星照片，偶尔附带罪犯的犯罪履历。难道是我们通过严谨的双重核查、数日乃至数周的观察，将罪犯的暴行与自身认定等同，从而自行授予了这种权力？我认为并非如此。[...]

真正的授权源于我们确信眼前这头怪物不配属于人类共同体——这个共同体不仅包含我这样的解放者，也囊括奴隶乃至那些通过剥削奴隶劳动来操纵世俗世界的统治者。那么，这个怪物必须被呈现在意外来客面前——因为他通过自己的所作所为，已将自己置于这个共同体之外。这是面对不可理解之事时，我们自我安慰的一种方式。

[image]

“这是一场冷酷的欢迎”（安德烈斯·特索帕斯特莱·特克皮莱，约翰·吉布勒）

以下内容摘自约翰·吉布勒所著《被世界撕裂：游击队员逃离墨西哥秘密监狱实录》。这本书于2018年以英文出版（西班牙文版首版于2014年发行）。

本书讲述了墨西哥游击组织"人民革命军"（EPR）成员安德烈斯·特索帕斯特莱·特克皮莱被捕、遭受酷刑及最终逃脱的经历。

1996年，安德烈斯遭墨西哥军方逮捕后被强迫失踪：他被关押在秘密拘留所，与外界完全隔绝，当局始终否认其被捕事实。

安德烈斯遭受殴打、电击及强奸威胁等残暴酷刑，却始终未向施虐者透露任何敏感情报。

历经数月折磨后，他成功逃离拘禁场所重获自由。

数年后，约翰·吉布勒在安德烈斯隐匿期间对其进行了多次访谈，本书即基于这些访谈内容撰写。

此处所述事件发生于安德烈斯逃脱数日后。他成功联络到人民革命军

（EPR）的战友，对方派人接应将其带至[image]藏匿点或安全屋 ，与组织指挥官会面。

安德烈斯描述了这场艰难的重逢：战友们对其逃脱拘留所的说法持怀疑态度，担忧他可能已被墨西哥军方"策反"，沦为双面间谍。斜体部分为访谈原话，其余内容由约翰·吉布勒根据访谈整理撰写。

安德烈斯的证词引发了关于信任、同志情谊的复杂思考，更触及如何接纳遭受酷刑的同志重返组织的问题。

有人来接你。他们带你去一座大城市。他们笨拙地用化妆品和假发给你伪装。在车上他们以惯有的冷漠和猜忌对待你。这是一致冷酷的欢迎。仿佛他们早就说出了这句话："你说什么我们也不信。"

抵达那个屋子时，你猜当时守候的人会如何迎接你？拥抱？欢欣？抑或猜忌？你无从想象。只知必须坦白一切。

墨西哥游击队*EPR*的指挥官奥斯卡和文森特现身。首轮审讯因猜疑而显得格外严苛："你告发了谁？你用多少钱赎回了自由？"

初始阶段你没有作任何抗争。不插话，不辩驳。有时甚至无法开口。尽管这正是你渴望的 —— 渴望有人倾听。但此处的氛围截然不同。

不仅是可理解的猜疑，连审讯的节奏与语调都不同。

你开始重温曾经的一切 ...

随后，负责分析你的专家到来，他们将判定你的言辞真伪。你被带去见心理学家和精神科医生，被灌下大量药物。而审讯仍在继续...

你渴望倾诉， 他们却将其转化为盘问 。仿佛他们将你从现场拽出后 ... 我是说 ... 不，不...... 他们给你拍全身*X*光片，三十多张，只为确

认体内是否植入微芯片。

比起关心你的健康状况，他们更在乎调查你是否"被跟踪"。

他们宣称："你身上没有明显伤痕，看起来也没挨过多少打。我们就是找不到证据。"

人们常说，酷刑幸存者脱离囚禁时往往浑身是血、肢体残缺，拖着一身烂肉在地板上爬行。这些人不明白，施刑者凭借其魔鬼般的、非人道的手段，早已将酷刑技艺臻于完美。这已非中世纪的刑罚。不，某些施加痛苦的方式从未改变…… 如今他们能用毛毯裹住你，用棒球棍击打而不留痕迹。他们能让你关节脱臼，却不必像中世纪那样将你绑在马背上。

尽管如此，你并不怨恨战友们。你没有仇恨。但你清楚他们无法理解这种伤害的程度，无法体会肉体对灵魂的殉难。他们缺乏这种深刻的良知。

[...]但你渴望他们倾听；你渴望诉说、诉说、诉说。可他们对你的每句话都挑刺。

当你讲述经历时，他们总打断道："不，你搞错了。感觉不是那样，而是这样。"

而你心底始终萦绕着同一个问题：你们可曾身临其境？他们告诉你："不，他们没想杀你，只是吓唬你。" 而你只想着：早说啊，混蛋们，我当时以为他们真要杀了我。

面对战友的冷漠与不信任，你心想： 此刻我只想让亲历者发声。真相不该被掩埋 。

这不该由我或他们来诠释。它只是段经历。无数经历中的一段，没错，但唯有我能讲述这段。

我所做的一切并非只为讲述或书写故事。历经如此苦难、如此猜疑、如此否认之后... 我不在乎。

我毫不在意，也无意辩解。为什么？因为不论说是这个或者那个，或是这场斗争，或是其他任何什么玩意 ... 统统去他妈的，我从来都不是叛徒，现在不是，将来也不会是。那不是我的梦想。

这就是一个反抗者必须面对这样的现实：要么胜利，要么在每个层面、每个维度、每个举动中彻底完蛋。 既然如此，我此刻便永远扮演者的角色。我认同这个身份，别无他选。

我别无选择。

我本不可能讲述这个故事，更不可能宣告：“我就是”。唯一确定的是，我并非为某个人而战，而是为另一个世界而战，为人类及其面临的一切而战。这就是我的遭遇。这场斗争是对抗犯罪国家，对抗杀人如麻的国家，对抗屠戮、灭口、杀戮的国家。

这很艰难。我创造、解构、拆解自己的形象。唯有我能掌控叙事方式以避免伤害。

因为单纯为了讲述而讲述，不仅令人不适，更充满痛苦。我认为每次讲述时，总有新的事物浮现——那些隐匿的创伤，或创伤的永恒存在，抑或所有伤痕的愈合。

我不会强迫自己说服你。或许你会认同某些内容，或其中部分片段，或某一天的片段，或什么都不认同，或全盘接受。我无法预知。我只是承受着。这是我理解的方式，说服他人并非我的职责。

不该……不该由我来解释。

我当然可以做到解释。是的，我可以回答你们这些荒谬的问题，容忍你们可笑的评论、种族主义的评判、你们的傲慢，以及你们虚构不存在事物的妄想。我本可以，但我不。这同样不在我的梦想之中。

[image]

后记（无痕计划）

阿尔弗雷多·博南诺在《不速之客》中写道，权力“本身就蕴含着驱使它诉诸屠杀与酷刑的迫切性”。我们认为此言不虚。军事独裁政权必须惯常施以酷刑以确保自身存续。民主政权若尚未惯常施刑，一旦感受到足够威胁便会立即效仿。地下组织同样难逃此劫：纳森·吉尔伯特·昆波因加入菲律宾共产党遭军方酷刑折磨九年后，该党武装组织据称在一次大规模"清洗"中酷刑处决了至少60名同情者。

因此我们主张，酷刑问题关乎所有渴望废除权威制度及其内在力量的人。

那么，该怎么做？

我们建议无政府主义者反对酷刑的首要步骤，是在自身处境中评估酷刑的风险与实施方式，包括：

1. 酷刑的筛选标准。被捕者是否遭受酷刑，可能取决于其涉嫌的罪名的性质、政治立场或疑似政治立场，亦或其族裔、国籍、性别认同或表达、性取向、宗教信仰等因素。

1. 酷刑的目的。尽管所有酷刑在某种程度上都旨在威慑受害者和/或第三方，但部分酷刑确系为逼供而实施，另一些则纯粹以制造恐怖为目的。

1. 酷刑的手段。手段选择取决于施刑者所奉的指令和其惯例，以及其是否有意在受害者身上留下永久性酷刑痕迹或致其死亡。

1. 酷刑的持续时间。酷刑可能仅限于逮捕瞬间，或集中发生于拘留初期数小时至数日，亦可能持续数周、数月乃至数年。

无政府主义者可据此评估制定个体与集体策略，例如：

1. 强化安全原则，如[image]信息最小化原则 和安全文化标准。同志应尽可能减少接触敏感信息，使施虐者难以获取可利用的情报。

1. 建立通讯协议，确保在同志被捕后能迅速获知消息，以便立即采取行动：
—— 保护被捕同志。在酷刑仅限于拘留初期阶段的特定情境下，逮捕后尽快向当局施压（例如通过律师或记者介入），可能有助于制止酷刑或减轻其严重程度。
—— 保护尚未被捕的同志，快速转移，，以防被捕同志"开口"。具体措施取决于被捕同志掌握的信息量，可能包括放弃[image]藏匿点或安全屋 、中止行动计划、或[image]隐姓埋名 转入地下活动等。

1. 做好心理准备抵抗酷刑。遗憾的是我们无法提供经验证实的准备技巧，仅希望本手册分享的见解能有所助益。

随后便面临一个更棘手的问题：如何对待那些在获释后遭受酷刑的同志 —— 无论他们承认还是否认在酷刑下"开口"，无论我们是否相信他们。

德米特里·彼得罗夫写道，那些开口的人"几乎不可能继续成为我们的同志和无政府主义运动的参与者"。安德烈斯·佐姆帕斯特尔·特克皮莱则揭示：当处境危急时，即使未供认也可能不足以保全，战友们仍可能不相信你。

[image]

我们也没有现成的答案，但我们愿意提出质疑：

- 能否采取更细致的处理方式？

- 能否在艰难情况下，让酷刑受害者参与其中，对每个案例进行伦理评估？

- 能否给予第二次机会？

- 当我们难以辨明真相时，能否在暂缓信任战友的同时继续陪伴他们，帮助他们疗愈伤痛和心理创伤 —— 即便他们暂时或永久地被排除在我们的行动之外？

敌人通过酷刑企图摧毁并孤立我们。如果我们能直面这些问题，岂不是更有助于避免这种毁灭与隔离、岂不是更接近覆灭敌人的目标？

在本合集序言中我们写道，酷刑是"是国家及其盟友在镇压无政府主义者的战争中常用的手段之一"。我们使用"战争"一词绝非轻率，正是在此框架下，我们收录了将刺杀施虐者视为应对国家暴力特定形态的有效手段的文本。重申一次，我们没有现成答案。我们只能鼓励同志们在各种情境中运用最佳判断力，并希望本合集能帮助大家更清晰地认识当前议题。

在此分享伊拉克作家、画家兼革命活动家海法·赞加纳的文字，摘自她记录政治迫害、酷刑与流亡经历的著作：

"悲伤是最初也是最终的归宿吗？
是粉碎梦想的元素吗？
痛苦啊，请退去吧，
让人在梦境森林中徜徉。
走廊尽头站着女孩，
她向太阳倾诉对黑暗的恐惧，
举起手指恳求我们每个人：
难道不该让希望重拾些许荣光了吗？"

—海法·赞加纳《梦中的巴格达》，2009年

愿力量与勇气永伴天下友伴！

[image]
[image]

别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命 S11E01

[image] 关键词	反渗透 告密 团队 战术 线人 防御
[image] 关联	[image]性、婚恋、密友…“反贼”如何构建亲密关系：战友爱侣 S10E01 ；[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；□告密者（线人） ；👹渗透者 ；[image]S11关系结构革命-总章节
[image] 创建时间	2025年11月2日
[image] Description	反渗透和协作；关系结构革命

[image]

返回：👹渗透者

返回：□告密者（线人）

返回：[image]“抓特务” 不是解决方案：整体安全S01E02- 威胁响应

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

渗透、告密、背叛，鬼气横生，草木皆兵……

想要对抗国家暴力机器主导的情报收集，仅仅揭露曝光是不起作用的。真正有效的方法是：创建一个更安全、更难渗透的网络。

本文就如何开始使您的关系网络更安全、和在日常活动和组织中创造积极的安全文化，提供一些建议。

- Table of Contents

  术语定义
  有五种基本的渗透者类型：
  第一部分：引言
  第二部分：构建更安全网络的实践层面
  构建您的工具箱
  安全指南：讨论篇
  创建基础安全圈清单
  创建网络图谱
  进一步调查的策略
  柔性提问
  尖锐提问
  物理检视
  案例研究
  与您的团队进行沟通
  与可疑人沟通
  当发现真正的渗透者和线人时该怎么办

[image]

术语定义

- 线人 ：被警方招募以提供情报的人员。

线人通常是被警方瞄准的团体内部的成员，或者其成员的朋友，以及有关联的人，比如家属或伴侣。

警方通常称其为“机密信源”或“机密线人”。

- 渗透者 ：以真实成员身份渗透进入目标团体的人员。

渗透者可能是军人、警察、职业间谍特工、黑手党成员、私人维稳承包商、或者五毛“爱国者”。

还可能是面临监禁的公民。

- 告密者 ：向当局提供可将目标人定罪的证据的人。

- “叛变案底” (Snitch Jacket)：指的是警方记录线人的档案。

该术语既用于警方行话，也用于街头俚语。该术语部分源于警方在审讯中对拒绝配合的被捕者进行威胁的策略 “如果你不配合，就把你写进线人档案里，让你的所有同志都知道你是个叛徒”。

- 网络 ：本手册中的“网络”指的是关系网络，由称为“节点”的个人（或组织）组成的社会结构，这些节点通过一种或多种特定类型的相互依赖关系相连接。

激进网络可能基于友谊、共享生活空间、共同兴趣、共同组织实践、组织成员身份、共享身份、性关系、以及与物理空间的联系（同城/邻里），等复杂链接。

【注一点题外话：是的，性关系也很重要，甚至可能更有凝聚力。这很可能就是为什么要终止“红姐”的主要原因。

城市社会的“原子化”一直在被普遍且广泛地描述（无国界地广泛），但其实这一描述并不准确。传统的家庭和亲属社会关系在城市中正在让位于其他关系：职业/企业关系、兴趣关系，或其他基于某些标准的关系。这并非“原子化”，而是亲缘结构的消退、并朝向利益/需求结构及其相应社会联系的转变。

“传统家庭”作为城市社会基本“单元”的解体进程相当迅速。正如大家都已

经看到的，婚姻和生育对年轻人的吸引力越来越低。到了第二代或第三代，与直系亲属的联系虽仍存在，但它们已不再主导城市居民所处环境的社会分层。这就是为什么婚姻状况和家族辈分的约束性越来越低；而类似“红姐”这样的通过解决实际需求而创建新关系结构的尝试，正在增多。

所以，如果仅仅假设镇压“红姐”的理由源于所谓的“性传统”等等，都是不准确的。这些东西与镇压当局唯一关心的社会稳定性和可控性并无直接关系，相反，真正具有挑战性的是“红姐”们生成了一套没有在派出所登记的、网格员不了解的社会关系结构，并且在某些条件下可能比登记过的那些关系更紧密。】

[image]

延伸：https://iyouport.substack.com/p/f2f?utm_source=publication-search

[image]

有五种基本的渗透者类型：

1. 闲逛者： 很少参加真正的行动，只热衷于参加各种会议、社交活动、收集文件、观察和倾听。

1. 沉睡者： 起初非常低调，几乎不可见，在某一事件/事态下忽然变得非常活跃。

1. “马仔”人设： 政治分析能力很低，倾向于跟随别人，甚至只是吹捧和模仿圈子里看起来有权威的人；长期致力于为自己建立信任和信誉（对被信任不足非常敏感）。由于跟圈子权威人物的私人关系热络，更容易实施挑拨和拉帮结派。这种情况尤其容易出现在等级制度明显的圈子中。换句话说，这样的人致力于搞关系，而不是搞志业。

1. ‘超级’活动家： 几乎无处不在，同时加入多个团体或委员会，作为组织者。跟普通积极分子不同的是，这种“超级”活动家几乎不会对项目的进展起到作用，相反他们更热衷于笼络权力和

人心。

1. 极端激进者：经常不合时宜地主张激进行动和暴力冲突。请注意“暴力/非暴力”不是道德问题，而是战术有效性问题；“不合时宜的暴力”主张就是战术有效性为零，而被抓捕的可能性百分百 - 延伸：https://iyouport.substack.com/p/ad0?utm_source=publication-search

---

渗透可“浅”可“深”。浅层渗透者可能持有假身份证明，但更有可能在周末回归他们自己的正常生活。浅层渗透通常发生在情报收集周期的早期，一定程度上这一阶段仍然处于对目标的识别过程中。

相比之下，深度渗透则需要24小时全天候工作，并且持续很长时间（期间也可能会定期休息）。他们可能拥有一份工作、一套公寓、一个伴侣，甚至一个家庭，作为渗透的一部分。他们会使用政府签发的假身份证件、工作经历和租房记录等。

[image]

第一部分：引言

首先必须明确的是，并没有万无一失的方法可以揭露卧底和线人。本手册探讨的是如何应对由警方发起的或协助的秘密间谍行动。

对抗国家主导的情报收集活动的目标并不是要追求将这些秘密行动公之于众（那是另一件事），而是要建立一个更安全的、更难以被渗透的关系网络，作为我们运作的基础设施。

讨论反间谍问题时需要谨慎，因为草木皆兵的氛围很可能导致人们去探索许多危险的、却事实上无益的或徒劳的途径。

显然，前线社区在反间谍方面的实践需要在理论和实践层面得到加强，以便我们能够在私人团体内部进行沟通。在过去几年中，各地的

激进网络中都出现了涉嫌或确认的间谍行为。无论是在法庭上、拘留室里、绞刑架上，还是在摆脱压迫和苦难的新世界中，我们都会意识到，只有我们自己才能组织自己的安全，只有我们的选择才能让我们为自由做好准备。

我们从对话起步。我们意识到，在激进环境中组织活动已使许多人接触过便衣特工。我们都曾批判性地思考过如何应对他们，一些人已经有过亲身经历、或者听闻过历史上前辈们如何应对类似状况的故事。我们来自独特的组织环境，我们的关系网络和警方调查行动都极其动态。对对话和个人反思的需求，以提供更大的保护给我们自己和我们组织出来的网络，已经成为一个不得不面对的难题。我们对自身关系网络发展和衰落的变迁进行分析，并将这些理解与其他激进网络进行深入沟通，是我们颠覆警察间谍行动的最有力武器。

📌

一份关于如何应对警方间谍行为的宣传手册需要解释渗透告密在警方更广泛调查工作中的作用。即，渗透者和告密者并非孤立存在；他们不是单打独斗的私刑爱好者。他们被部署在特定调查中是为了收集情报、构建针对目标个人的案件，并可能破坏整个网络的效力。

如果您的关系网络中存在渗透告密，要知道，他们是更大规模调查的冰山一角。类似这样的调查通常（尽管不总是）包括详细的监视行动、诱导和操控者，以及负责更加技术层面的情报人员。

来自北美的真实案例：在最近一起卧底警察行动中，据透露，该卧底警员始终与另外两名警察保持密切接触，而且被渗透的激进网络中还有其他成员在场。他们还有一名联络员，每天早晚与之会面，以审查笔记并制定每日目标，且参与监视行动的警察数量远不止此。

此外还有各种类型的秘密特工渗透并动摇了激进组织。简而言之，有浅层和深层两种渗透形式。线人包括那些深入激进运动并决定倒戈、协助建案的人，已经在压迫压力下投敌的昔日盟友。这些笔记仅涉及进入激进网络的线人和警察，不包括国家证人和那些与组织建立长期信任关系的深度线人。

如何构建绝对不受告密者、越界者和国家证人影响的网络，这一问题需要 在不同情境下从根本上加以探讨 。

保护您的安全就是保护每个人的安全。无政府主义动员活动的目标是建立一种社会力量，这种力量有潜力通过团结来摧毁等级制度和范式。其他目标包括：建立基础设施和自主空间，干预冲突，推动紧张局势升级为革命，以及实现我们个人和集体自由的潜力。无政府主义者揭示，自由主义的个人自由概念建立在对他人的支配与冷漠的基础之上，而作为无政府主义概念的个人自由无法与集体分离，但只能由个人定义。这一理念在进攻性斗争中得以体现，团结精神是反权威斗争的核心。例如在温哥华攻击警察，是对圭尔夫或其他地方面临同样压迫制度的人们的直接团结和声援。通过这些进击，削弱警察作为社会道德执行者的不可动摇性，对于提升我们的集体能力和自主性以对抗他们这些国家机器，从而夺回自治权，具有深远影响。

在类似的层面上，我们组织自身提升能力以有效抵御条子内鬼的渗透操纵，同时保持住社会存在，与我们对自由的理解紧密相连。我曾听过那些刚刚遭受渗透告密毁灭性影响的人说："要吸取的教训是，我需要与那些我不信任的人保持距离，并与我熟悉的人合作开展项目。" 问题在于，如果仅仅将间谍行为视为对个人自由的威胁、只一味自卫，会导致我们的人际关系网络暴露在攻击之下。相反，如果我们能对关系网中的所有联系进行细致调查和批判性的审查，而不是让自己抽身，我们就能为整个网络和自身都提供更大的安全保障。互助和团结的行动能强化我们每个人，这些行动保护我们，并可以使我们更具进攻能力且难以被操控。

"让条子渗透进来呗，他们可以为我们做饭洗碗嘛。他们不会得到任何东西，我没什么好隐瞒的。"

[image]

仍然有一种相当普遍的观点认为，如果网络内部的保密文化与外部世界保持良好隔离，渗透进入的便衣警察并不会真正损害网络。即，让警察渗透进活动家团体，或者如果你担心某人，让他们以边缘的方式参与，只要他们不靠近核心，就没什么问题。这种观念源于自大的想法，认为具体的激进分子是渗透监视的中心目标。这种逻辑没有考虑到，对反权威抵抗网络的刑事调查不仅旨在将激进抵抗定为犯罪，还

旨在动摇和削弱整个反抗网络，并创建社交关系档案。

无政府主义者对渗透告密的放任态度源于懒惰，不愿扰乱团队的稳定状态，不愿让自己看起来像是那种会把条子放在眼里的懦弱者，更不愿让自己看起来像是在背后说三道四的人，也缺乏进一步调查他人背景的工具，感到无助或被孤立，可能还有其他原因。有这些情感和理性是人性使然，但最终它们会导致最危险的状况。在未被清除出关系网络的情况下，渗透者会通过人际关联建立信誉，对每个人建立详细的社交关系档案，寻找压力点、以在网络内部制造紧张和冲突，诱捕团队成员，从我们的舒适圈内部监控我们的日常生活。

最后一点：您的关系网络中可能存在让您感到不适的或干扰组织工作的个别成员 —— 类似这里的案例。他们未必从一开始就是秘密特工，但仍需组织者直面问题，或者将这类人从组织角色中移除，以确保安全或提升网络功能性。尽管目标可能不同，但此类关系对网络的破坏性影响与真正的渗透并没有根本性区别，并建议公开讨论类似事件。

[image]

第二部分：构建更安全网络的实践层面

> “感谢您教导我们，面对权力，唯一注定失败的战斗是从未开打的战斗。” —— 迭戈·里奥斯

我们参与讨论、阅读信息并研究激进网络内部遭受镇压的历史，至少部分是为了从中汲取可应用于现实生活的实用经验。以下是尝试制定的一套讨论指南（可能不完整），可根据需要调整并应用于您当前的网络。

简言，这里列出了一些普遍适用的建议，这些工具可能有助于个人努力构建更坚实的安全基础。

构建您的工具箱

- 了解并研究来自卧底、线人和告密者的不同类型风险。
- 研究历史案例中关于卧底、线人和告密者对社会运动和地下组织趋势造成的实际影响。
- 查阅相关警察文献，了解警方的调查技术，以洞察卧底警察行动可能的运作方式，并开发针对性的对抗措施，以增强安全。
- 查阅与安全文化相关的文献及当前讨论。
- 考察不同时代和地区激进网络、革命组织所采用的组织方法，并将其与当今无政府主义网络基于亲密团队的组织模式进行比较。
- 历史案例研究：OCAP、Os Cangaceiros、Rote Zora、A.L.F/E.L.F、红军派、爱尔兰共和军、黑豹党、起义无政府主义、自治运动以及二战期间被占领的欧洲的反法西斯抵抗运动。

或阅读以下书籍：

- We Are An Image Of The Future
- The Subversion Of Politics
- Agents of Repression: The FBI’ Secret War Against the Black Panther Party and the American Indian Movement
- Black Mask & Up Against The Wall Motherfucker

- Argentina’s Anarchist Past: Paradoxes of Utopia
- Confronting fascism: Notes On a Militant Movement Direct Action

安全指南：讨论篇

“击中直线飞行的鸟儿，易如反掌。” -B. Gracian

以下是为进一步讨论而制定的六部分安全指南，旨在构建更安全的网络。不存在单一的解决方案。本模型可提供建议，以引导更安全的实践。最终，这些构建更安全网络的结构化方法必须保持高度动态性，以令其持续保持实地有效性。随着警方渗透战术的适应性调整，我们的应对实践必需相应调整以保持领先。

六个部分是：

- 创建基础安全圈清单
- 创建网络图谱
- 进一步调查的策略
- 与您的基础安全圈沟通
- 与可能的渗透者/线人沟通
- 采取行动

创建基础安全圈清单

创建一个参与您所在网络的人员调查清单。

通过一系列结构化问题，评估您与网络中每位成员之间的安全等级：

- 谁是与您关系密切的人？
- 您是如何认识他们的？
- 谁是您的战友（与您实际合作项目的人）？
- 谁是您可能与之发生冲突的人？
- 他们与您有何历史关联？
- 你们是如何相识的，在哪里相识的？
- 通过哪些人介绍认识的？
- 您是否见过他们来自不同社交网络的其他朋友？
- 您是否见过他们的家人？
- 您信任的人能否验证他们的背景？
- 他们生活中有哪些方面是您难以沟通或验证的（工作、家庭、车辆、过去的经历）？
- 您是否已经与您共同合作的项目中的组织人员清楚地谈论过意图问题，并且对他们感到满意？
- 他们是否与您讲述过与您熟悉的经历类似的经历？您对他们的

描述方式满意吗？

- 您是否对他们有强烈的信任感？有没想过原因是什么？

您现在会得到两份清单。对于其中一部分人，您对上述问题回答得游刃有余，并感到非常安全和信任：这就是您的安全基础圈。名单上的其他人，您可能对他们了解程度不一，但他们生活中的一些方面或与您相处的方式可能让您感到疏远。您希望在将他们加入安全基础圈之前与他们进行更多沟通。

您会意识到，彼此的了解和安全感可能会形成一个层次结构，其中一些人可能只需要简短的对话就能感到更安全，而另一些人可能需要付出很多努力才能建立安全感。

从个人层面来说，这样的调查清单是我们日常在心理上做出的社交选择的正式延伸。这项练习旨在提升我们对与之交往的人做出明智且批判性选择的能力。这些评估问题的目标是批判性地理解构成日常互动的社交关系，以及您通常所处的更广泛社交网络。以这种方式分析关系，不仅可以映射和实现相对安全关系网络，并且，可以帮助揭示您希望进一步了解谁、了解他们的哪些方面，从而有望推动他们成为您的关系网络中更安全的联系。

使用此类练习可帮您奠定安全基础，并允许进行主动的个人研究，最好在相对平静的时期进行 —— 而不是在出状况的混乱情况下。花时间和精力完成这项工作，是朝着与安全相关的批判性和赋权选择迈出的重要步骤，这些选择能帮助您的团队从偏执的无助和恐惧中挣脱出来，重新夺回自主权。

创建网络图谱

将您所在的关系网络中的人员列表放置到网络图谱上。使用3种不同颜色的笔在图谱上写下人名，具体取决于他们是否属于您的安全基础圈，或是您希望在将其添加到安全圈之前进一步了解的人。

颜色1) 安全基础圈。

颜色2) 需要稍多沟通的人。

颜色3) 需要大量沟通的人。

现在，使用更多颜色来画线，创建链接，以揭示关系网络中人与人之间的感知联系。

颜色4) 共同居住的人。

颜色5) 在网络中与您最亲近的人

颜色6-?) 使用记号笔尽可能明确地定义具体项目的成员关系。例如，一个颜色的标记用于连接您当地的无政府主义反战组织的成员，另一个颜色标记用于定义入狱者支援团队，等等。

请注意：切勿把秘密组织活动纳入此列表。

您完成的图谱将揭示以下细节：

- 图谱中某个人在关系网络中的嵌入程度，由他们拥有的链接数量和类型决定。
- 呈现网络中人们之间存在的社交关系类型。

它可能揭示……

- 您希望加强沟通的某人，可能也与您的安全圈中的其他人关系密切。

- 与您的安全圈中的其他人组织合作的人，可能与您存在松散的社会联系。

- 您是否需要您的安全圈中的其他人协助进行这项调查？

进一步调查的策略

把您想要进一步增进了解的人视为潜在的安全圈成员（而不是潜在的卧底）至关重要。如果您认为无论如何都无法对该人存在于您的关系网络中感到安全，那么问题可能不仅仅是缺乏可信度这么简单了。万一真的出现这种情况的话，建议与安全圈中的亲密朋友讨论解决方案，例如考虑将该人移出网络，或者与对方坦诚沟通为何不愿与其合作。（推荐后者方法）

柔性提问

柔性提问旨在以隐晦的、不易察觉的方式提出问题，其目的是在不暴露提问者意图的情况下了解到一些事情。

考虑环境和氛围，并尝试控制提问时的环境变量。一个放松且舒适的人更容易让对话者放下戒备。他们更可能配合您以维持对话的愉快氛围。当人们处于压力状态时，也无法察觉肢体语言和面部表情的变化。

围绕您希望了解的他们生活方面提出微妙且无害的问题，会有所帮助。例如，如果您想更好地了解他们的过去，可以在友好的对话中将话题先引导到您的家族历史，并提出诸如这样的问题：“你的口音听起来有点像我妈妈啊，我妈妈是A省人，你去过A省吗？”

尖锐提问

尖锐提问具有质询性。旨在让与您交流的人感到紧张，让他们知道您

对真相是认真的。

这适用于可以即时验证的问题。比如，你出生在哪里？在哪里上过学？你的生日是什么时候？你以前从事什么工作？给我你父母的电话号码，然后和我一起在这里等，我来验证这些信息 ……

物理检视

- 车牌号和车辆识别号（VIN）
- 地址（垃圾箱潜水、造访 ...）

案例研究

在美国东海岸，一次信息自由请求导致一名线人的身份被揭露。激进社区通过调查努力，缩小了搜索范围，并对一名潜在的线人进行了监视，直到确认其渗透者身份。

在匹兹堡，G-20峰会前夕，所有参加会议的人都填写了一份简短的问卷。当有人无法充分回答问题时，他们被要求离开本次会议，或者直接离开激进网络。

在欧洲某些激进网络中，人们在加入网络之前常会被要求提供与本人亲近的人的电话号码及其他验证信息。

通过安大略省交通部进行车牌查询，可能揭示车辆所有者的身份，以及该车辆是否租用的、或者政府部门的、或属于与执法部门合作的维稳公司的车辆。

在圭尔夫进行的与布伦达·道格蒂作为当地大学学生身份验证相关的研究，可能早在2009年9月就已暴露其卧底身份。

与您的团队进行沟通

告密现象可能在反权威网络中普遍存在。我们需要建立一种安全模式，通过收集信息、并以避免恐慌避免耸人听闻的方式进行沟通，以尽可能限制偏执的滋生。

所有沟通方式都是基于具体情况的，这些建议基于个人经验和反思，不确保适用于所有情况。每位使用者都可以随时根据您的具体经验进行更新。

与网络成员的沟通的重要性与敏感性均不容小觑。安全问题往往会激发出人们内心深处的非理性、挫败感和不安情绪。讨论“你认识的人可能出于恶意目的在操纵和欺骗你”这类话题，很可能会引发网络内部的强烈紧张和分裂。

根据我与潜在卧底进行对话的经验，亲密朋友之间总会因如何处理此类问题（甚至是否处理它）而产生强烈分歧与挫败感。基于此，建议您在展开对话前，先思考下如何缓和可能引发分裂的谈话内容。沟通的起点应从基础层面的柔性提问开始，逐步深入调查，或考虑将相关人员纳入您的基础安全圈。

认真思考如何向您最亲密的战友、与您正在调查的人最亲近的人、尤其是您感兴趣的个人，透露您掌握的信息，目标是零容忍八卦和伤害性谣言。良好的沟通目标，如同对抗国家主导的间谍活动的目标一样，其本质并非揭露秘密活动，而是要建立一个更安全的、更难被渗透的网络。这种对个人和集体安全的渴望，比永无止境地抓特务更具建设性。

[image]

与可疑人沟通

- 中文俗语说的很对，“一人为私，两人为公”，这就是为什么国家暴力机器总是成双成对出现。渗透者也是如此。您应该注

意，如果渗透者就在您身边并且正处于工作状态，那他们很可能并非独自一人，无论是携带录音设备还是有未被察觉的其他便衣条子在场。

- 在提出指控前请等待确认。要记得，误判造成的损失可能比错过更大。

- 注意您对话的方式，即便您已经持有确凿证据可以揭露渗透行为，也要小心，要有深思熟虑的计划，以避免被倒打一耙。“威胁警员”正成为一种更常见的指控。

- 要谨慎，不要透露意图，始终保持平和的友好的态度，可能比审讯式沟通更适合获取真相。

当发现真正的渗透者和线人时该怎么办

“我们必须说话，尽管说出来可能导致暴露我们所有的缺点和弱点 —— 因为承认弱点并坦率地说出来，本身就是一种力量的象征。但不要刻意、不要夸张，而是偶然地、不经意地，说出来。” —— 赫尔曼·梅尔维尔

By 美国无政府主义杂志发行商“萌芽”

[image]
[image]

为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力

[image] 关键词	交往 人际安全 反渗透 告密 女权主义 线人 组织
[image] 关联	；[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；告密者（线人）
[image] 创建时间	2025年12月30日
[image] **Description**	反渗透和协作

为了挽救我们的运动，我们需要认识到性别暴力、男性特权与条子线人（以及表现出类似告密行径的人）用来破坏激进运动的策略之间的联系。

- Table of Contents

线人是如何养成的
对激进运动中性别暴力的简要历史反思
性别暴力的种族政治
遭遇左翼的厌女症：个人反思
展望未来：在我们的运动中创造性别公正

[image]

iyoupoŗt: 本项目将在未来开设关于激进派/和异议社区内部如何处理和尽可能减少性暴力/侵犯行为及类似程度的人际冲突的专题，以及，对如何通过革命性的组织结构打破屏障以构建变革项目和合作的具体战术问题进行探讨。关于反渗透（避免抓特务式的混乱内讧）这一议题我们将放在今年的主要工作 “Phase II” 中作为一个专题出现。

本文在我们近期主持的小范围研讨活动中采用，现分享给所有朋友，并附上我们粗略挑选的部分参与者的观点，这些观点反应的是参与者的个人经验和认识，IYP对此不做任何评论。

A：一些自由派分不清什么是自由开放、什么是滥交卑贱，他们故意混淆这两者，是为了他们自己可以随意把侮辱当亲热。而左派的七寸就是“大局为重”，甚至不惜损失原则来保全战略（坦克党形成的逻辑之一），最终瓦解“大局”的就是那些被忍让忽略的“附带伤害”。

我觉得华人进步派社区还有很多基础级的功课需要做，比如，通过培训教会更多人如何把“女权”和妇联区分开、把团结和服从区分开、把辩论和捣乱区分开 …… 把性爱和剥削侵犯区分开。（我是直女）

B：有时候人们可能会奇怪一些性暴力/性骚扰受害者为什么会在很多年之后才说出真相，为什么她们不能在第一时间直接反击？有人认为她们害怕侵犯者的势力和威胁，这样认为的人就会倾向于相信米兔运动能够帮助受害者减轻恐惧。但事实上不完全是那样。一些侵犯者以虚构的爱情和伪装的政治共识来骗取对方信任，一次甚至多次侵犯后会继续假装恋爱关系足够长的时间，然后再慢慢甩掉。他们可以同时对多个人这样做。其中每个受害者都在很多年之后才会意识到自己被骗了。这就是为什么她们不可能“第一时间”说出来，并且米兔倡议不起作用。

一直以来我们只是在普及如何反击，我觉得这是不够的。我们需要首先让更多人理解到什么是爱。流行的说辞完全被父权的等级压迫价值观所占据，混淆了很多人的认知，什么霸道总裁式、舔狗式、爆金币式等等，其实爱并没有什么“式样”之分，只有爱还是不爱之分 …… 支配文化中、等级制度中、“主权”规则中，都不可能有爱。这些都是和爱相悖的东西，无法共存。有些错误是本质问题，而不是方式问题，模糊判断可能导致灾难性后果 ……

我觉得这些小册子应该在各地的信息商店占据重要位置，而不是等待某些节日或搞活动的时候再拿出来推广，因为它不是某个“议题”，它是基本价值观，是原则层面的问题，父权等级制是统治者的价值观，采取统治者价值观的人怎么能自称“反贼”呢？（我是酷儿）

𝒞：说到反贼，我觉得很多人有误会。现如今窝在微信群聊里的某些人，不客气的说，仅仅是看清了党国的穷途末路想要转身押注下一个主子而已，他们心里最关注的东西是自己的股票行情、自家的不动产保值、鸡娃的竞争力、如何花最少的钱润出去然后在圈子里吹牛，而不是你们所想象的反抗运动，解放就更谈不上了。我并不是在批评自私，自私不是问题，有些时候自私还能成为最直接的策动力。我说的是价值观问题，他们的价值观与党国基本一致。

这些人很可能支持变革，但那不过是因为他们是党国体制的受害者，现政权没有让他们发财，所以他们头脑中的变革基本只是相当于换个主子。在这样的群体中厌女恐同和物质主义才是最普遍的价值观共识。如果你用自由平等的价值观在这里判断和筛选是不是“战友”的话，你很快会发现基本剩不下几个人了。所以这不是下雨打伞这么简单。除非你能从组织战略、从组织结构上以最充分的方式体现革命性和解放斗争的总方向，然后在此之上寻找同道并组织起来，否则目前的绝大部分问题都无从解决。（我是直男）

𝒟：摆脱父权价值观不是容易的事情，尤其对男性来说，特别尤其对精英主义男性来说。他们从小就被绑定在各种竞争机制中，唯一的规则就是要么夺冠要么出局，他们是在这种威胁恐吓中长大的。这样的人很难接受和内化平等价值观，也基本没有被平等相待的经验，连模仿的机会都没有。这样的人容易被操纵毫不奇怪。

我亲眼见过的代表性案例就包括，仅仅为了炫耀自己的所谓“人脉资产”就将该“人脉”的私密交谈内容随意暴露给其他人。这样的人简直是天生的告密体质，都不需要警察费力收买。这是有多可怕。

如果一个人的价值观接近统治者，不论其是否明确为警察线人，其所作所为都只能令统治者受益。价值观是能杀人的。（我是非二元）

ℰ：俗话说“知书达礼”，人们总是下意识地给读过书的人贴上“明白人”的标签。但事实经常会能让你大跌眼镜。学历越高越接近制度的受益人，就越是难以真正理解反叛（反叛不是异议、甚至超越反对派/反对党）。这就是为啥准精英阶级大多是改良派，他们不颠覆任何东西，甚至可能都没能完整想象颠覆这个概念真正要表达范围。

能从精英教育里走出来抵达真正的反叛位置的人，才是绝对的高手。

读书人最大的优势应该是学会反思，学会质疑自己被灌输的东西，学会前进。否则被体制吸收掉真的太容易了。（我是酷儿）

F：我始终支持“说出来”。任何时候“说出来”都是自强的反抗。

但是，如果我们只是满足于“能说出来”，满足于被安慰、被同情、甚至被怜悯，把罪责和对共识原则的背叛行径转变成了我们自己的自我感动，我们就等于给了不公正以更大的生存空间。

仅仅“说出来”不会让任何事情发生改变；我们通过陈述事实是希望动员人们意识到激进社区整体结构中存在的漏洞 —— 而不是某一两个人的所谓“私德”，意识到所需的结构性变革及其重要性 —— 而不是拉一群人来吃瓜。（我是直男）

……

iyouport: 以上选择的只是少数代表性观点；还有更多精彩发言，感谢所有参与思考的朋友！**IYP**将平等和尊严的福祉视为安全性问题的重要部分之一，因为只有这样大家才能轻松协作并共同前进。我们将在今年的项目二期工程中详细介绍应对和改善的策略。

[image]

2009年1月，得克萨斯州奥斯汀的活动人士得知，他们中的一位名叫布兰登·达比的白人活动家作为联邦调查局的线人渗透进了抗议共和党全国代表大会（RNC）的团体。达比后来承认在战术策划会议和大会期间佩戴了录音设备。

在2009年2月对两名得克萨斯州激进派活动家的审判中，达比代表政府作证，两名活动家在RNC大会上被捕，罪名是“制造和持有自制燃烧弹”—— 而燃烧弹正是达比所鼓励的。

这两名年轻人分别是戴维·麦凯和布拉德利·克劳德，两人都因此面临长达15年的监禁。

克劳德接受了认罪协议，在联邦监狱服刑三年；在联邦检察官的压力下，麦凯也被迫承认持有“未注册的自制燃烧弹”，并被判处四年监禁。

达比作为警察线人收集的情报可能也服务于RNC八人案的审理，他们是来自全国各地的活动人士，被控 “共谋暴乱和共谋破坏财产以助长恐怖主义”。

奥斯汀的活动家们对达比担任警察线人的消息尤其感到震惊，因为他曾参与过各种左派的项目，并且是 “共同救援/CG” 组织的领导人。CG组织是一个位于新奥尔良的组织，致力于满足墨西哥湾沿岸地区因自然灾害而流离失所的社区成员的短期需求，并致力于重建该地区，确保卡特里娜飓风撤离者的返回权。

我也曾一度对这一消息感到惊讶，但我并不觉得意外。我在德克萨斯大学读本科时就知道，校园警察局经常安排便衣条子渗透进激进派学生团体的会议 —— 你知道，就是为了监视他们。

那是在2001年的秋天。我们目睹了国安局的成立，看着牛仔总统发动“反恐战争”，当时我们都在努力试图弄清楚可以做些什么以挑战在我们眼前发生的法西斯国家政变。

然而，在当时看来，警察线人跑来参加我们的会议似乎很傻 —— 我们并不是 “黑豹” 或 “棕色贝雷帽” 那个级别的激进运动，甚至我们的激进程度远不如校园里另一些直接行动反全球化的活动家（尽管我们都很钦佩他们）；我们只是一些不相信战争是对 9/11 袭击“最好回应”的年轻人。但这并不愚蠢；联邦调查局绝不会忽视政治工作。

⚡

任何组织，无论规模大小，都可能引起国家的关注。只要国家认为你的组织构成了巨大的威胁（换言，你们的战略目标具有颠覆能力），不管你们目前的规模是否较小，但总有一天你们会成长起来，大到国

家机器无法控制的程度。国家通常会选择在运动发展壮大之前将其扼杀在摇篮里。

线人和煽动者 是国家雇佣的枪手 。政府机构 会挑选一些 通常没人会注意到的人来做线人。也就是说一般情况下无法证明他们是线人的那种人，因为他们看起来完全致力于社会正义。他们与前线社区建立亲密关系，成为活动家的朋友 甚至恋人 ，还经常在组织中担任领导职务。

粗略阅读一下20世纪六七十年代有关社会运动和组织的文献就会发现这一事实。美国印第安人运动的领导层充斥着警察线人；人们怀疑线人就是黑豹党垮台的主要原因，同样可以推测20世纪60和70年代的反战运动也是如此。正如阿萨塔·沙库尔（Assata Shakur）、伊莱恩·布朗（Elaine Brown）和罗克珊·邓巴·奥尔蒂斯（Roxanne Dunbar-Ortiz）等活动家的自传所表明的那样，曾经那些被告密者和挑衅者推翻的运动同时也是女性和酷儿活动家经常遭受强烈性别暴力的场所，这一点不足为奇。

也许，并不是告密者难以发现，而是我们集体忽视了暴露他们的迹象。

为了挽救我们的运动，我们需要认识到性别暴力、男性特权与条子线人（以及表现出类似告密行径的人）用来破坏激进运动的策略之间的联系。

一次又一次，激进运动中的异性恋男性被允许维护他们的特权并压制他人。尽管我们说了很多相反的话，但事实是，美国的激进社会运动和组织拒绝认真对待性别暴力，没能认识到这是对我们斗争生存的威胁。【 我用“性别暴力”一词来指恐同和厌女植根于异性恋对性别认同和性别角色的理解。异性恋主义不仅限制“非正常”的性行为，还复制了规范的性别角色和身份，强化了父权制和男性特权的逻辑。 】

人们通常将厌女症、恐同症和异性恋主义视为 “较小的邪恶” —— 次要问题，认为一旦“真正的”问题 —— 即 种族主义、警察、阶级不平等、侵略战争 —— 得到“解决”，所谓的“小问题”最终会自行解决或淡出背景。选择无知会带来严重后果。厌女和恐同是激进活动家社区

内部暴力再现的核心。挖开一个厌女者，你会发现一个恐同者。再挖深一点，就很可能会发现一个未来告密者的潜质（或者像告密者一样破坏运动的人）。

线人是如何养成的

在 Democracy Now! 节目中，马利克·拉希姆（Malik Rahim）作为前黑豹党成员，也是新奥尔良 “共同救援/CG”（Common Ground）项目的创始人之一，在谈到达比被揭露是FBI线人后他表示自己有多么地震惊，他多次提到自己的心都碎了。他特别惋惜那些因达比的专横跋扈、咄咄逼人的组织风格而离开CG项目的 “年轻女士们”。

这些 “年轻女士们”抱怨的是什么呢？好吧，她们的担忧很可能落在了同情者的耳朵里，但最终却没有得到真正的回应 —— 一切可能都是真的，事后每个人都承认那个达比是多么具有破坏性，他很快就提出了暴力的、完全考虑不周的直接行动方案，这危及到了与他共事的每个人。

甚至还有人声称，达比曾经对CG项目组中的女性组织者进行性侵犯，而且对在该组织工作的女性普遍不屑一顾。【我在奥斯汀和新奥尔良参加 “奥斯汀线人工作组”时，与曾经和达比合作过的女性活动家的非正式交谈中了解到这一点。】

达比擅长挑拨，在他工作过的所有组织中都制造过冲突，但人们却总是念着他作为组织者的资历、以及他对 “工作”的 “奉献”，而迟迟不愿追究他的责任。

人们继续为他辩护，直到他坦白自己是联邦调查局的线人。

即使是拉希姆，出于他的愧疚和焦虑，也选择让达比负责CG，尽管组织中的每一次冲突似乎都与达比有关。

也许，如果组织者能将性别暴力的集体问责作为我们实践的核心部

分，我们就能让那些代表国家破坏我们斗争的人失去作用。

⚡

我说的绝不是猎巫，而是以这样一种方式组织起来，在潜在的类似达比这种线人伤害更多人之前将其扼杀在萌芽状态。正如贝尔·胡克斯（Bell hooks）所言："无风不起浪，无论走到哪里都会制造混乱的人，要么是受雇的线人，要么是根本上的不负责任、不靠谱的定时炸弹，在破坏社会正义组织方面，捣乱的人可能无意中导致与线人一样的后果。归根结底，他们都在为国家暴力机器做事，他们都需要因此承担责任。

[image]

对激进运动中性别暴力的简要历史反思

对二十世纪六七十年代激进组织和社会运动的反思为本次讨论提供了重要的历史背景。

安吉拉·戴维斯（Angela Davis）、阿萨塔·夏库尔（Assata Shakur）和伊莱恩·布朗（Elaine Brown）在她们加入黑豹党（BPP）的不同时期，都将性别歧视和黑豹党对妇女（及其组织劳动）的剥削作为她们离开黑豹党（布朗和夏库尔的情况）或拒绝正式加入黑豹党（戴维斯的情况）的主要原因之一。尽管人们常常期望妇女做出重大的个人牺牲来支持这场运动，但当女性成员发现自己受到男性同志的伤害时，她们却得不到任何支持，也没有寻求补救的渠道。

无论是黑豹党组织者无视埃尔德里奇·克利弗殴打妻子 - 著名活动家凯瑟琳·克利弗 - 的事实，还是男性胁迫女性发生性关系，抑或是男性将女性组织者视为从属的性玩物，黑豹党和类似组织往往不重视性别暴力对解放斗争的腐蚀作用。在许多方面，伊莱恩·布朗的自传《权力的滋味》最深刻地揭露了运动中厌女现象的丑陋现实，以及在这些组织中的男性和女性都以各种方式再现并强化了男性特权和性别暴力。

作为领导黑豹党的唯一女性，她的经历并没有使她免于该组织残酷的厌女症。她讲述了自己被各种男性同志（包括休伊·牛顿）殴打的经历，以及被埃尔德里奇·克里弗殴打和恐吓的经历，后者曾在一次前往中国的代表团活动中威胁要将她 “埋在阿尔及利亚”。

与戴维斯和夏库尔的传记相比，她的传记更明确地展示了黑豹党（以及当时许多激进组织）的大男子主义姿态如何创造了一种暴力和厌女的文化，而这种文化最终被证明是该组织的致命伤。

这些叙述揭开了我们许多人所仰慕的激进组织所遗留的性别暴力的神秘面纱。它们展示了厌女症是如何在这些组织中被正常化的，是如何被视为 “个人”行为/所谓的“私德”、或者被认为不如反对种族主义或阶级不平等的斗争那么“重要”。

性别暴力在左翼的政治实践中历来根深蒂固，是对这些组织生存的最大威胁之一（如果在很大程度上没有得到承认的话）。但如果现在的我们开始关注戴维斯、夏库尔、布朗等人的著作，我们就能避免过去的错误，创建不同类型的政治社区。

性别暴力的种族政治

种族问题进一步复杂化了我们社区中性别暴力的蔓延方式。

雷切尔·卢夫特在《寻找共同点：飓风后新奥尔良的救援工作是美国种族和性别暴力的寓言》一文中，探讨了2006年在上第九区进行重建工作的白人男性志愿者对白人女性志愿者进行性侵犯的令人不安的现象。她指出，CG组织未能解决白人男性对其合作的组织者的攻击问题，而是将责任推给了周围的黑人社区，并警告白人女性活动家“需要小心”，“因为新奥尔良是个危险的地方”。最终，事实证明，将附近的黑人男子定罪要比承认白人女性和非二元组织者最有可能受到与她们共事的白人男子的攻击要容易得多。

在一个案例中，一名白人男性志愿者在一周内性侵犯了至少三名女性，之后才被移交给警方。白人男子在CG这个表面上致力于种族正义

的组织中享有特权，这意味着他们可以对女性和酷儿活动家施暴，做出扰乱组织工作的破坏性行为，而且他们知道，组织不会像对他们工作的社区中的黑人男子那样追究他们的责任。

当然，男性的特权并不是千篇一律的 —— 白人男性和有色人种男性都是父权制的不平等参与者和受益者，尽管他们都可以也确实在复制性别暴力。当我们试图对抗在我们社区中实施性别暴力的有色人种时，妇女和酷儿组织者并没有忽略父权制利益分配的这种不平等。我们经常担心会复制特定类型的种族主义暴力，而这些暴力过多地针对有色人种男性。

可以理解的是，我们都不愿报警，不愿让国家以任何方式介入，不愿让有色人种受到历来具有种族主义色彩的无法无天的刑事系统的摆布；但我们的社区（不论是纯政治社区还是其他社区）往往不会站出来为我们伸张正义。我们不愿意与治疗师交谈，因为治疗师主张向内归因 - “谁痛苦谁改变” 反而把责任推给我们。左翼立场也经常不支持我们，用他们的话说就是，我们的受害经历是不幸的、是有问题的，但最终对 “大局” 的重要性来说不如那些在我们的社区中繁衍暴力行径的各种族男性。

[image]

遭遇左翼的厌女症：个人反思

在我积极参与的第一个社区团体中，我遇到了一种以前从未想象过的厌女情境，在一个本应是激进的有色人种组织中竟然存在这种厌女症令人惊讶。

我与团体中一位年长的奇卡诺活动家发生了性关系/恋爱关系。我当时19岁，是一个没有经验的年轻黑人活动家；他30岁。他让我对我们的关系保密，我勉强同意了。后来，在他结束这段关系后，我陷入了抑郁，我发现他和我在一起的同时还至少在和另外两个女人上床。其中一个女性还是我的朋友，另一个也是我们组织中的年轻姑娘。后者不知道我们之间关系的性质，他没有向她透露，她和他睡在一起，直到他消失，拒绝接听她的电话、拒绝解释他们的关系突然结束的原因。

在分享了我们的经历后，她和我开始与其他认识这个男人并和他一起合作过的女人交换各自的经历。

我们听说，一些女性离开了一个墨西哥裔学生团体，在团体参加墨西哥城的萨帕塔运动时，他的谎言和秘密被揭穿，之后她们就再也没有回来。还有一名酷儿、激进的白人组织者离开奥斯汀，以逃避虐待。还有一名白人女性，一名社会工作者，她一度以为自己会和那个男人结婚，但一天晚上她来到他的公寓时，发现我在那里。还有其他一些人来找我。我一直想知道他们是否知道他的真实身份。他约会过的女人都是了不起的、美丽的、出色的、激进的女人，他利用她们作为他自己的护盾，将自己带入一个他知道永远不会对这样一个厌女者开放的地方。

但他对女性的厌恶还不止于此，还体现在他的组织风格上。在会议上，他总是发言最大声、时间最长，使用的学术术语让任何讨论都复杂得令人难受。这种学术用语让教育程度比他低的人望而生畏，让他显得似乎比其他人更了解激进政治。他会居高临下地对小组里的其他人说三道四，尤其是那些他认为不如他聪明的人，基本上每个人都是如此。然后他会换个话题，为自己主宰了这个空间而道歉，并承认他需要检查自己的男性特权。

具有讽刺意味的是，当人们试图骂他的时候，他会假装无辜 —— 被说大男子主义和性别歧视，这能是什么意思？他会抱怨自己被幼稚化了，却拒绝看到自己是如何一直幼稚化别人的。

他本人也是有色人种，在种族主义和种族正义斗争问题上可以论述得头头是道，但这一事实掩盖了他在激进组织和个人关系中的虐待行为。正如他的一位前合作伙伴与我分享的那样："他激进的种族理论分析让人们（大多数是男性，偶尔也有女性）原谅了他在人际关系中的支配性和虐待行为。女性甚至不得不进行自我检讨，反思自己对他行为的批评是否客观，“以免我们在运动中失去一位有色人种”战友。让有色人种男性对性别暴力的繁衍负责之所以如此困难，原因之一就是有色人种女性和白人活动家仍然认为有色人种男性比其他人“更艰难”—— 当一个人被贴上标签是“国家暴力的头号目标”时，谁还敢去追究他的责任呢？

不幸的是，这类情况在激进社区里甚至都不是罕见的。他只是其中比较聪明的一个。

回顾以前的电子邮件，我对其中一些与我一起组织过的男人所发的电子邮件的内容感到震惊，其中有很多带有粗鲁的语气和内容，他们很容易因为别人犯了一点小错误而贬低对方。更让我吃惊的是，我像一个遭受虐待的幸存者一样，试图去安抚那些认为对自己的伙伴、朋友和其他组织者大吼大叫“没有什么不对”的同伴，但我的反应却温顺得像个外交官。在我工作过的各个组织中，都有这样的人。在我们主办的夏季聚会上，有人当着一群有色人种青年的面骂他的女朋友是婊子。那个在墨西哥旅行期间性骚扰一对墨西哥裔同性恋情侣、还试图迫使他们玩3P的人。那些说要完成任务却不去做的人，对同伴的问责要求不屑一顾，让其他女队友接手任务，而任务完成后却把别人的辛勤劳动全部归功于自己。那个打了自己伴侣的研究生 —— 大家都知道是他干的，但每当有人问起，大家都会一脸羞愧和尴尬，喃喃自语："这很复杂”。 那些不断贬低同性恋者的人，甚至还有不少专门针对有色人种队友 ……

对，就是这些人。

⚡

这些人中的大多数可能并不是受雇的警察线人，这甚至更尴尬，因为这意味着他们所做的破坏性工作和受雇线人一模一样却得不到一分钱的报酬。我们可以把这些厌女症看作是国家的无心之举。无论他们是否真的是线人，他们所做的事都支持着国家对社会运动和创造这些运动的人们持续不断的恐怖活动。当酷儿组织者受到羞辱、他们的政治斗争被搁置一旁时，这是国家针对激进分子的持续暴力计划的一部分。当女性被故意感染性病、遭受身体虐待、在会议中被忽视、被排挤到一边、被迫离开激进组织空间，而我们的盟友却在为众所周知的厌女者辩护时，就意味着运动的组织者在国家摧毁我们的努力中与国家暴力串通一气。

国家暴力机器早已明白这个左派一直难以接受的事实，即：厌女者是很好的线人。在他们被国家招募来扰乱运动或破坏组织稳定之前，或者不管他们是否被招募来扰乱运动或破坏组织稳定，他们很可能已经精通扰乱行为的做法。他们几乎不需要任何培训能直接上岗。他们通过各种暴力、拉帮结派和勾心斗角将我们中最好的女性组织者和酷儿

活动家挤出会议、压制后者的影响力，导致后者被迫离开社区，导致我们整个工作乃至整个运动陷入瘫痪，还有什么比这更具破坏性的？或者，当你不得不推迟关于工作的谈话，以便将小组会议用于处理个别成员最近的冒犯行为时；或者当这个人散布谣言，在激进团体中制造混乱和摩擦时 …… 没有什么比厌女者更能减缓运动的发展速度了，因为父权制的本质就是权力争夺。

警察们非常明白这点，当激进分子中有人致力于争权夺势，并将权力理解为统治时，整个运动都将永远无法实现其重塑世界的潜力。相当于自我镇压。

如果我们的精力都被线人（和那些像线人一样行事的人）制造的混乱所占用，我们将永远无法专注于真正的工作、获得自由，建立我们想要生活在其中的那种以人为本、肯定生命的社区。用贝尔·胡克斯的话说，只要存在支配的意愿，就不可能有正义，只能是城头大王旗，因为在支配文化中所有人将不可避免地继续复制我们声称要反对的那些不正义。

现在是我们的运动从内到外进行彻底变革的时候了。

[image]

展望未来：在我们的运动中创造性别公正

变革运动无法承受性别暴力带来的破坏。如果我们低估了社区中父权等级制行为的政治影响，这项工作将无法维系下去。

最近，我一直在研究酷儿/有色人种女权主义者的作品，那些经历过被大男子主义削弱的社会运动混乱局面的女性活动家的自传。我正在重温贝尔·胡克斯（Bell hooks）、邓巴·奥尔蒂斯（Dunbar-Ortiz）、托尼·凯德·班巴拉（Toni Cade Bambara）、爱丽丝·沃克（Alice Walker）、奥德雷·洛德（Audre Lorde）、希奥孔达·贝利（Gioconda Belli）、玛格丽特·兰德尔（Margaret Randall）、伊莱恩·布朗

（Elaine Brown）、珀尔·克利奇（Pearl Cleage）、恩托扎克·尚格（Ntozake Shange）和格洛丽亚·安扎杜阿（Gloria Anzaldúa）等人的著作，想要学习其他女性是如何在这些空间中协商性别暴力的，并对暴力如何在我们的社区中繁衍提出整齐或简单的答案。

并且，除了书本之外，我们还有很多资源可以用来应对这一困境。说出并分享大家各自的经历和遭遇是我们能拥有的强大的工具之一。我一直在与我的长辈、经历过我正在与之抗争的事情的年长有色人种女性交谈，并与其他女性幸存者交换经历。

2008年夏天，我开始与奥斯汀的劳工组织者和作者克里斯蒂娜·津佐一起举办关于终结厌女症和建立集体问责形式的研讨会。我们还开始了一种更加自由的做法，即公开说出我们的经历，并呼吁社区解决我们和其他许多人所经历的问题。

消除厌女症不能仅仅由女性来做。我们所有人都必须做这项工作，因为我们运动的整体生存有赖于此。

除非直接挑战保守的组织形式和结构、将酷儿反叛政治伦理作为政治实践的核心，否则激进运动将继续被布兰登·达比这类警察线人（以及那些尽管不是受雇于警察，但其表现得像线人一样具有破坏性的那种人）的滑稽行为所破坏。

我们需要认识到性别暴力是如何在我们的社区、人际关系和组织实践中繁衍出来的。尽管有许多方法可以做到这一点，但我想建议我们可以从以下三个关键步骤开始。首先，我们必须支持运动中遭受过人际暴力的女性和非二元战友，和他们一起参与集体疗愈过程。其次，我们必须开展集体对话，讨论大家希望我们的社区是什么样子的，以及如何使社区对每个人都安全。第三，我们必须建立一种集体问责模式，真正将个人视为政治，帮助我们开始在社区中践行正义。

由于被错误使用而导致非常令人反胃的一句流行语声称“谁痛苦谁改变”，在革命者社区中这句话会带来灾难性影响。当你眼看着女性和酷儿组织者为了保护被暴力欺辱的同志不得不离开活动空间而沉默不语时，就等于是在说你更看重那些搅乱社区空间的警察线人，而不是那些一直在奉献精力建设整个运动的人。这一立场非常可怕，一旦先

例，后患无穷。

尽管左派社区内部存在性别暴力这一事实让我愤怒，但我也没有失去希望。我相信我们有能力改变并在我们的运动中创造更多的正义。我们不必通过抓特务那类猎巫行为去揭露厌女者和渗透者。

每当他们拒绝道歉、拒绝对自己的行为负责、拉帮结派挑起冲突、并拒绝通过协商解决冲突、言语和/或行为暴力虐待同伴时，他们自己就已经暴露出来了。不要去审查彼此，不要“寻找”问题，但当看到破坏性的行为时，必须能立刻反应过来，并追究责任。我们的策略不必是惩罚性的，人们有权犯错；但是，我们应该期望人们能够为自己的行为负责，不要让有错不纠变成一种模式。

革命者是预示政治行动者，我们要建立的社区本应成为一个更美好的、更公正的世界的典范，如果我们的社区里庇护着同样的恐同、厌女、种族主义暴力行径，我们每个人都有权感到愤怒。为了拯救我们的运动，我们需要正视性别暴力、等级制特权和渗透告密（以及与他们行为相似的人）用来破坏激进运动稳定的策略之间的联系。

作为激进运动的组织者，我们必须相互问责，不能让厌女者在这些空间中拥有如此大的权力。不允许他们成为这些运动的代表、发言人和领导者。不允许他们强奸同伴，然后一转身就在他妈的热点新闻上装腔作势。在布兰登·达比的案例中，即使没有人怀疑他是线人，他本人的专横跋扈和大男子主义行径也足以应该让周围人质疑他的领导能力。

通过不允许厌女症在我们的社区和运动中扎根，我们不仅能保护自己免受国家破坏我们工作的努力，还能创建更强大的运动，使其无法从内部被摧毁。

🖊 作者考特尼·D·莫里斯是激进社区活动家，也是加州大学伯克利分校性别与女性研究副教授。

□

[image]
[image]

卧底警察识别手册2025版

[image] 关键词	个人 判断力 反渗透 反间谍 团队
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病
[image] 创建时间	2025年12月31日
[image] Description	反渗透和协作

渗透者是如何被识破的？是否存在识别他们的方法或公式？如何开展调查？如何判断我们认识的人或组织成员是否为卧底警察？……

本手册针对启动调查时可能遇到的各类问题，提供信息指南、常见模式分析、操作建议及防范渗透的安全措施。

- Table of Contents
按
手册
谁撰写了这份手册？
目标是什么？
所有这些真的适合公开吗？
为什么说由调查小组掌控调查过程至关重要？
1、出于保密考虑：
2、出于时间管理考量：
3、出于自身利益考量：
为什么我们要在调查中成为积极的政治主体？
怀疑
你产生过怀疑吗？
做好被事实推翻的准备
做好找不到答案的准备
调查小组

职业倦怠
调查过程
如何调查受怀疑的对象？
1. 写下怀疑的理由
2. 评估初始怀疑
3. 整理数据
4. 证实或排除怀疑
5. 联系或吸纳更多人加入调查组
调查结果
1. 证明其并非渗透者
2. 无法确定
3. 如果你是对的……
经验教训和后果
如果你发现身边潜伏着渗透者，该怎么办？
相互支持
调查阶段提供情绪支持的经验教训
偏执倾向
结语
研究材料
案件资源
调查工作中最常使用到的关键问题
1. 此人是否没有生活背景？缺乏社会根基？
2. 此人的政治观点是否很模糊、或者不够成熟？
3. 有没有人见过此人的家人？
4. 工作或“个人”生活是否导致此人长期或频繁短期失踪？
5. 此人的住处是否看起来冷冰冰的缺少人气？
6. 他们是如何进入组织或社交圈的？
7. 是否有超凡的驾驶技术或持有多种驾驶执照？
8. 他们的态度或性格如何？
9. 钱方面是否不明不白？
10. 社交关系是否集中在核心人物身上？
11. 是否检测到任何怪异或矛盾之处？
12. 是否出现过离奇的诉讼撤销或警察缺乏兴趣的情况？
13. 是否突然消失并切断所有联系？（脱离/撤离）
14. 社交网络
15. 照片
重要数据特征
成员加入组织前的可行（/但非万能的）筛选机制

是否存在“红线”？—— 渗透者不能干什么
结论

[image]

按

首先请注意区分渗透/卧底、和线人/告密 —— 在本站的相关教程中这两者是有区别的。在这里看到简单介绍：[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01 。

华语异议人士经常将所有可疑人员简称为“特务”，这种简化不是不可以，只是可能不利于防御。良好的防御需要您更准确的了解威胁模型和风险机制。

简单说，渗透者通常是指“外人”，他们确实供职于镇压机器，而且他们从来都不是单枪匹马的，其背后通常会有一个战术小组随时指导行动。使用渗透手段的情况意味着目标组织已经涉及了一个“案件”，此案件正在“侦查”阶段；或者，目标组织的结构和/或其战略中心特别吸引镇压机器的兴趣，后者正在想办法“制造案件”。

线人则始终都是目标组织的“内部人士”，他们以各种不同的方式被镇压机器拿捏住了把柄，从而被操控为镇压者的耳目。当然，线人也不是“单枪匹马”的，但不至于必需一个战术小组来接应，相反，顶多一两个警员作为“所有者”与其密切联系，并指挥其行动。线人的使用可能服务于特定案件侦查，也可能由于线人的告密而导致立案。甚或，纯粹是为了捣乱和制造恐慌，都有可能。比如华语地区有关于“占坑”的传说，即网格维稳系统在民间组织/团体形成的最初即混入线人。不论真假、不论覆盖面，这类传说本身就增加了系统性的恐慌。

所以，相比下，实施渗透对于镇压当局来说成本更高 —— 这里不仅有协调成本，还有培训成本和雇佣成本。线人则成本较低。并且鉴于人们通常对新人/陌生人更多警惕、对熟人/“自己人”放松警惕的倾向，线人长期存在的威胁性事实上更大。于是对于镇压者来说，采用挑拨离间的方法发展线人比安插专业的渗透者的可能性更高。

一般情况下可以认为，线人的比重可能比渗透者大，对大多数民间组织和团队来说，也包括激进派组织，都是如此。

而相比下，倾向于采取渗透手段的情况包括：

- 目标组织门槛很高，内部凝聚力很大或无法掌握，该组织也没有显著的等级制度或者权力关系不明显。这种情况下发展线人会比较困难，可控性难以保证。比如以种族血缘身份为基础的组织、机构、自治政府等。

- 目标组织零门槛，流动性极大，没有等级制度，激进程度很高，专业性和成熟度都很高，组织形式类似亲密团队，但较少发展人际纽带，而是基于具体项目的联合。如黑客主义团队等。

- 可能较高激进程度、临时且广泛招募的行动小组，例如应对一些时效性的行动项目，如战争和灾害（供应链和交通封锁、罢工、罢课……等类似行动招募）。这类行动本身也是积累亲密团队人际网络的重要基础。对镇压当局来说可能是方便的渗透入口。所以说亲密团队需要秉持安全文化。

强调：这不是百分百绝对的！对镇压当局来说，战术选取取决于很多因素，如政策风向（是否需要“杀鸡”）、便捷程度（手头的预备役情报线索是否方便）、时间窗口……等等。这就是实战经验需要起作用的地方 —— 希望前线资深活动家多多分享经验以帮助新人更快掌握分析方法。

在华语区，我们甚至听说警方在高校中“物色和培养”情报人员，以备长期使用。其背景可能是对学运的历史性高度警惕，借助党建网络的高覆盖面与大数据侵入性监视的结合。这类“被培养”者可能有多种不同的学科背景，并没有清晰的警校经历，其身份“底子”干净，不容易识别。同时，甚至很难说清这类人究竟是受雇的渗透者、还是被威胁出卖朋友的线人，更准确地说应该叫“内线”，镇压系统对他们的“使用”方式可能相当灵活；加之，利益和威胁可能并存，其受雇证据不容易获取 …… 这些都是需要警惕的地方镇压风格。

也许有人会觉得，“如果我们只是在讨论问题，而没有任何具体行动，那我们就不必担心渗透了”？不是的。别忘了有一个最常用的罪名曰“煽动颠覆”（在其他国家可能被称为“阴谋罪”），在此，执法者可以掌握超大的解释空间 —— 可以直接对整个组织结构采取镇压、无需任何实际行动的“证据”，可按需扩大执法范围，尤其是在需要完成维稳指标的情况下。

更何况，为什么要把自己的发展前景直接堵死呢？越是艰难时代越应该对勇气和机动性保持自信 ...

以下是手册正文。

[image]

手册

> "我曾听闻，当蚁群迁徙至需渡河之处时，走在前面的蚁群便会集体跃入水中，层层叠叠地溺毙，以自身躯体为后方同伴架起桥梁。" —— 小林多喜二《自己的蚁丘及其他无产阶级故事》

谁撰写了这份手册？

本手册由亲身经历过警方渗透的活动家撰写，这些渗透行为发生于2022至2024年间并被揭露。本手册面向所有过去、现在、及未来的活动人士，以及所有以任何形式关注自身空间安全的组织和团体。

目标是什么？

我们在撰写本手册时设定的目标如下：

1. 传递我们在应对警方渗透行动时积累的经验和知识 —— 这些正

是我们此前缺乏的应对能力，包括如何预防类似的渗透侵害。

1. 提升组织和团体的安全意识。

1. 向行动者传递关于警方与国家机器的明确信息：他们并非无懈可击，事实可证。其运作机制存在漏洞，我们旨在以公开透明的方式揭露这些缺陷。

所有这些真的适合公开吗？

在撰写本手册前，我们审慎的权衡了所有方案，内心存有疑虑：是否应该公开我们掌握的这些信息，包括在每起已揭露并公布的渗透案件中获取的情报？如果此举危及正在进行的调查该怎么办？如果警方从此改变了渗透手段，又当如何？

我们权衡了公开此类文件的所有利弊，同时参考并评估了英国在这方面的经验，最终得出以下结论：

1. 我们认为必须公开迄今揭露的此类案件中所有尚未公布的已获取信息和数据。显然，这里所指的绝非那些可能不必要地暴露我们、且对实现目标毫无裨益的病态煽情细节，而是真正有助于理解这些镇压手段运作机制的核心问题。公开这些信息极有可能帮助众多组织发现潜伏者、和/或消除潜在的嫌疑。

1. 如果只有少数人掌握如此重要的信息，意味着我们只能将其传递给亲近的和/或受信任的组织，从而助长了“人人自扫门前雪”的个人主义和裙带关系。这小部分人承担着调查可疑事件的全部责任，使我们背负着在后勤层面根本无法承担的压力与工作量。如果将此事全权交由我们的判断与意志处理，不仅危险且缺乏保障，更可能滋生显著的等级制度与权力滥用。

1. 显然，警方已经了解这些调查，仅从媒体目前发表的文章来看，他们就能发现我们正在调查的所有案件中存在的共同模式，这些模式有助于我们完善对渗透者运作方式的理解。仅凭

这一点，他们就可能正在考虑改变警务策略（如果他们还没有这样做的话）。或许在本手册发布之后，他们就会做出这样的决定。那么，为什么我们还要发布它呢？

一方面，可看到英国和西班牙警方的渗透战术极为相似，且已沿用数十年。换言，国家拥有行之有效的运作模式（相关事实可供查证），因此改变策略意味着放弃成功模式冒险尝试缺乏保障的新方案。这具有不小的成本。

另方面，当前是否存在一个所有活动家都能使用的、内部可访问且足够安全的渠道，以确保信息不落入警方之手 —— 包括潜伏在活动家中的可能卧底？遗憾的是，这个问题的答案显然是否定的。

公开这份文件的另一潜在弊端是可能危及当前针对渗透者的调查。确实存在这种风险 —— 一旦潜伏的渗透者知晓自己正被调查，或至少意识到某些手段已被曝光，他们可能逃离。如此，我方组织中便少了一名卧底警察；如果其滞留，我们则有很大机会将其擒获。

无论如何，我们权衡利弊：一方面，我们担心公开文件会影响一项或多项调查；另方面，所有行动者都值得且应该知道如何识别潜在的渗透者。我们认为，显然应该选择后者。

此外，促使我们决定公开这份手册的另一个原因是英国的经验以及我们与他们就此问题进行的对话。当我们询问他们是否进行过类似的内部讨论时，他们表示确实进行过，但最终还是决定公开这份手册。我们也想知道，数年后回望时，是否能看到这项工作带来积极的影响。他们给了我们响亮的肯定。这份文件的公布，使得我们得以发现更多曾接触过该文件但与我们毫无关联的组织内部的渗透者。别忘了，如果这份文件几年前就落到我们手中，我们的队伍被渗透的持续时间或许会大大减少。

一个团队或群体不愿公开存在卧底警察的事实可能有多重原因（羞耻感、自尊心、“家丑”、缺乏管理能力或手段等等）。事实上，尽管这种隐瞒看似情有可原，但其唯一后果是加剧了我们的团体和环境的不安全感，导致无法从这些案例中获取宝贵信息 —— 这些信息本应该可以帮助我们发现镇压机构的行事规律，从而揭露更多渗透案件、并

获取更多行动工具。

[image]

在多起国家警察渗透社会政治运动（住房运动、反种族主义运动、反法西斯运动等等）的案件曝光后，活动家和组织会有诸多疑虑：他们是如何被识破的？是否存在识别他们的方法或公式？如何开展调查？如何判断我们认识的人或组织成员是否为卧底警察？

我们将基于自身经历尝试解答所有这些问题。

虽然我们稍后会详细讨论，但遗憾的是，证实这些怀疑绝非易事：目前没有公开的便衣警察数据库，即便存在大量不利于他们的证据，要想把证据收集起来也需要经历漫长的调查过程。

为什么说由调查小组掌控调查过程至关重要？

1、出于保密考虑：

- 如果涉案人员并非警员身份，在确定渗透行为之前传闻的扩散可能严重损害当事人的形象和声誉，很可能难以挽回，并造成当事人的心理情感伤害。
- 如果涉案人员确实是警员，一旦被TA知道自己正在受到调查，就可能会采取行动（如转移视线、销毁证据、实施报复等等）。

[image]

近似的防御原理：[image]信息最小化原则

2、出于时间管理考量：

不依赖他人，不受迫于取得成果的压力等。

3、出于自身利益考量：

不否认诸如《La Directa》和《El Salto》等替代媒体在揭露卧底警察的所有案例中一直都在发挥关键作用 —— 它们既能让发现卧底的活动人士保持匿名，又能作为揭露渗透行为的扩音器。但有时相比下我们的目标和运作方式可能存在差异，因此必须由这个初始调查小组来掌控时间节点和信息发布。

为什么我们要在调查中成为积极的政治主体？

多数案件的调查都是基于环境中的可疑迹象而启动的。我们能够也必须采取行动。我们拥有独立调查这些可疑迹象的手段和能力，无需依赖他人，同时赋予其恰当的政治视角，并始终服从于斗争利益而非其他任何利益。我们深知，未被揭露的渗透者会转移到其他集体和集会中。因此，在可疑案件中，我们负有调查、揭露并采取行动的政治责任。

仅凭怀疑是不够的，因为怀疑本身永远不足以成为传闻的理由。如果存在确凿的怀疑，调查小组有责任提供可靠的证据来支持其主张。我们必须避免在没有进行充分调查的情况下妄加指控。这种未经必要核查的行为可能导致团体瓦解，并造成无法弥补的政治与个人损害。

本手册针对启动调查时可能遇到的各类问题，提供信息指南、常见模式分析、操作建议及防范渗透的安全措施。其中大量内容源自西班牙近期的实践经验，以及英国过去十年间总结的有效应对策略。

[image]

怀疑

你产生过怀疑吗？

从这个问题开始讨论该话题似乎有些奇怪。但探究周围人产生疑虑的起点和诱因通常可以是一个很好的切入点。我们绝不会无缘无故怀疑一个人，通常是因为某些令人不安的迹象或某种异样的感觉。

作为行动者，我们不仅要提升理论能力和动员力，同时也要培养观察和分析环境的能力；在某些情况下，我们还会对周围的人产生一种直觉。大多数怀疑始于对细节的观察：对方的穿着风格、政治观点、社交圈、缺乏根基的表现、生活经历中的空白，或者仅仅是因为此人显得格格不入。但是别忘了，社会和政治运动可以吸引各种性格的人，因此这个层面的怀疑可能很多，而且往往都是毫无根据的。这里强调的是，识别这些疑点何时以及为何开始，可能对我们很有帮助。

另一种怀疑来自于阅读曝光渗透案件后的“事后审查”。也就是说，在几个月甚至几年后才意识到，某位（前）同仁的行为竟然与卧底模式如此吻合 —— 尽管他们曾是非常优秀的活动家，参与过大量行动（包括一些激进的非法行动），而且在共事期间，你“敢发誓”他们绝不是渗透者。

此外，在西班牙和英国的案例中，还有一种非常常见的情况：某位同志（后被证实为渗透者）突然、意外、且莫名其妙地离开了组织，理由通常是严重的家庭问题（亲属生病）或工作变动（换工作、调职等等）。

无论你有什么样的怀疑，这都是一个有效的起点。但我们要意识到，任何怀疑都仅仅是起点。正如本手册中反复强调的那样：我们描述的模式中哪怕有多项吻合，也不能证明任何问题，因为其中许多特征在我们这类圈子里是非常普遍的。别忘了，渗透者的所有行动都是为了融入现实、不引起怀疑，所以他们的表现甚至可能显得平淡无奇。

产生怀疑后如何行动，才是最重要的。

[image]

返回：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

返回：[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

做好被事实推翻的准备

如果对某人的行为或过往产生了怀疑，这并不意味着对方就是内奸。人们隐瞒过往、行为反常或突然消失，往往存在诸多正当理由。我们必须以开放心态开展调查，并做好被现实推翻预判的准备。

[image]

能够为他人"洗清嫌疑"，远胜于证实最坏的猜疑。

开展调查时应秉持这样的信念：与其直接预设最坏结果，不如期待调查结果呈正向，

即便最终证明自己判断有误。

如果以"对方必是内奸"的固执信念启动调查，却发现事实并非如此，你将陷入徒劳的证明困境 —— 试图证实虚假的指控，其危险后果是毁掉对方的声誉，也难免毁掉您自己的信誉。有时调查没有发现不利证据，仅仅是因为“证据”本就不存在。

做好找不到答案的准备

警方卧底的世界本质上充满隐秘，各方都在竭力维持这种暗箱状态。

世上没有能提供明确答案的魔法。目前发现的警方卧底案例属于例外，而非常态。

其中被发现的人，是偶然契机与周遭疑虑、系统漏洞及叙事破绽共同作用的结果。

在英国，曾出现过调查多年依然没有确凿证据或清晰答案的情况。

未来所有准备进入这项工作的人都应该做好心理准备。

调查小组

我们的经验表明，来自多个独立个体的怀疑最值得重视（拉帮结派的小圈子不属于这种情况，那其中的个人都不是独立的）。正是通过这些集体的怀疑，我们才能组建起密切合作的调查小组。“独立”至关重要 —— 只有确保独立才能避免单个成员说服他人将微弱怀疑视为“确凿证据”的情况。

群体内部的制衡机制往往能发挥作用：当某人对某项行为或状况产生疑虑时，如果由更了解当事人或情况的人进行解释，就更容易化解疑点。

团队启动调查时，需要从一开始就确立指导原则，比如：可就该问题与哪些人沟通？如何确保保密性和谨慎性？如果疑虑得到证实或被证伪，将采取何种措施？

调查一个你一直视其为战友或朋友的人，这绝非易事。因此，引入一个值得信赖但与被调查者没有直接关系的人来指导调查小组，可能会很有用。这个人可以扮演不同的角色，例如确保过程不偏离轨道、通过承担部分责任来帮助成员管理情绪，或者在调查行不通时帮助关闭调查。

同样重要的任务是质疑假设、并批判性地审视证据，例如帮助团队避免高估自身掌握的证据量，以及警惕草率下结论的风险。

尽管个人也能完成这一过程，但有研究经验的人士普遍意识到，在团

队协作中推进工作会更有利。

职业倦怠

不幸的是，在这种情况下，倦怠感非常普遍。这是一种很少被谈论也很少能得到正确处理的情感。

这种疲惫通常与失控感相关，甚至演变成某种强迫症。反过来，这会导致失去大局观，看哪里都觉得有威胁。“偏执”是常见的表现，可能导致针对任何言行稍有出格者的“猎巫式审判”。

[image]

听从直觉和陷入偏执之间只有一线之隔。这也是通常首选团队合作进行调查的另一个原因，因为倦怠的症状更容易被合作者察觉到并因此有机会得到处理。

[image]

调查过程

如何调查受怀疑的对象？

1. 写下怀疑的理由

这是一个虽小但不可低估的步骤。

花时间写下怀疑的具体原因有助于理清思路，明确让你担忧的重点在哪里。这也有助于评估恐惧的本质，并向小组其他成员展示你的疑虑。分享信息并对比记录。

写下你对该人的所有了解，特别是最初引起你怀疑的地方。

目标是获得尽可能 广泛的视角并增加透明度 。

2. 评估初始怀疑

接下来的部分基于国家警察多年使用的技术。通过分析已被揭穿的渗透者，我们制定了这份文件并重构了他们使用的大部分模式。

研究方法的结果被浓缩为 17 个基本问题和我们正在处理的更多数据。虽然这些问题可能在各种背景下都有用，但答案主要基于 2022 年至 2024 年间在西班牙和英国揭露的渗透案件。

您可以将这些问题应用于您自己的怀疑对象，或者以此为起点。如果某人“符合”其中很大一部分特征，那么怀疑很可能是有根据的，但您仍需要进一步深入调查以确证。

3. 整理数据

随着调查的展开，清晰地整理信息（例如按主题）。绘制时间轴、地图、联系人列表、该人可能出现过的事件和地点。寻找时间轴上的空白点，并列出可能了解情况的人员名单。

明确掌握已知信息和待查信息是必不可少的，特别是在小组协作时。

花必要的时间去核实并记录你所听到的内容以及是谁说的。请记住，有些人和组织不希望自己的名字公开出现或与渗透事件联系在一起，但他们提供的信息可能至关重要，我们应设法将其纳入调查。同时要评估来源的可信度，人们的怨恨或偏见可能会影响他们的记忆。

请记住：妥善保管你的资料！ 想象一下，如果被调查的人其实不是渗透者，或者这些信息落入警方手中破坏了调查，会造成多么糟糕的影

响。

4. 证实或排除怀疑

这一阶段本质上必须做到详尽彻底：调查当事人陈述的每一个方面，寻找蛛丝马迹和矛盾之处。其目的在于确定此人展示的身份是否真实，或者相反，我们面对的是否为使用虚假身份的渗透者。

回顾迄今为止已曝光的渗透者资料非常有帮助，这能让你知道应该关注哪些细节。但请记住，每个案例都是不同的，某些方面可能比其他方面更重要，经验只做参考，不要完全照搬。

其他需要核实的事项包括：可疑者在活跃组织之外的生存痕迹，以及他们的个人背景、就业经历等是否属实。你可以尝试通过追溯他们的过去来证实其存在：他们是否真的在所说的学校就读过，是否在所说的地方工作过，等等。

出生日期始终是一项重要信息。在我们经历的案例中，假身份的出生日期通常与真实身份一致。此外还有关于童年、家庭、工作等等私人故事。渗透者利用“真实”生活的细节来增加故事的可信度并不罕见，尽管这些细节的价值高低是相对的。在某些案例中，这些信息片段起到了决定性作用，而在另一些案例中则几乎没有影响。很难预料哪些重要，哪些不重要，因此最好记录下所有的一切。

这通常是一个缓慢排除可能性的过程。问题的核心在于确定某人是否是一个“幽灵”——即一个看似存在，但当你试图调查其过去时却消失得无影无踪的人。

5. 联系或吸纳更多人加入调查组

当你认为疑虑需要进一步证实时，可能就得找其他认识此人的人谈谈了。这一步需要格外小心：你接触的人必须知晓调查小组的约定，并理解该过程的敏感性。

要意识到，你接触的人可能会感到愤怒、震惊或断然否认。为此要做好充分准备，既要防止你的怀疑被直接回绝导致局面失控，也要避免在没有进一步调查的情况下仅凭怀疑就导致人员身份曝光。

确保为新加入的人提供处理这些消息的空间和支持。在这一步，你应该明确事情目前仍处于调查阶段，尚未得出结论。同时还应强调保密协议的重要性。

当你怀疑的对象可能是某些人的好友甚至是伴侣时，解释起来必须非常委婉。每个人的反应各不相同，我们无法预见情况会如何发展。但我们与警察和国家的一个关键区别在于，我们对同志负有责任感，即使与他们在政治上存在分歧。此时，你应该考虑为自己和他人准备好可能需要的心理支持。

让小组内每个成员都能表达具体的个人需求，并始终保持信息互通，明确谁在做什么。

洞察每个人愿意贡献的程度。有些人可能希望参与所有环节；另些人则可能担心调查工作耽误其他政治活动，但他们仍对决策感兴趣。此外，还有一些问题需要注意，比如平衡不同的需求（例如隐私保护与采取行动之间的平衡），以及应对倦怠和精疲力竭的风险。

[image]

调查结果

调查不太可能产生绝对确凿的结果。只有在挖到卧底警察的真实姓名时，才能达成百分之百的确定。

在某些案例中，有机会彻底开盒是由于该卧底自己的疏忽大意造成的——比如丹尼的案例，他把一个U盘交给了另一位活动家，以为自己已经删除了之前储存的信息；结果对方成功恢复了他身穿警服在阿维拉国家警察学院的照片，以及他跟其他警察同事的合影等等证据。在其他案例中，则是依靠调查小组持续追踪所有可能线索和开展深入调查的能力，才得以揭露卧底身份的。

以下列出了调查可能出现的几种结果：

1. 证明其并非渗透者

[image]

在最理想的情况下，我们能够消除对该成员的怀疑。

但仅仅得出结论并认为到此为止是不够的 —— 必须向所有讨论过此问题的人传达结论。

我们坚持认为，不能通过影射或任由谣言持续来毁灭一个人的名誉。

此外，还必须决定是否告知被调查者本人。

对于某些人来说，这代表了一种需要评估的透明度，但另一些人可能会对此反应非常激烈。有些小组决定干脆不提调查的事，但要注意这可能导致流言蜚语长期挥之不去。

根据怀疑在人群中散播的广度，这个问题以后可能还会被再次提起。

请记住，如果搜集的材料落入别有用心的人手中，这些信息可能会被用来对付被调查者。因此，如果证明怀疑是错误的，请务必彻底销毁曾经搜集的一切信息。

2. 无法确定

警察渗透、内线、告密者、秘密情报员和私人间谍的世界本质上是非常阴暗的。它由国家机器运作，拥有专业的手段和机制，他们始终会尽一切可能隐藏活动并制造掩护。我们中许多人也可能有正当理由不愿完全公开自己的过去或个人史。如果再加上我们的政治运动日益内化了安全文化和对他人隐私的尊重，我们就会发现，识别卧底警察确实非常困难。

如果你怀疑某个曾经或正在参加集会或团体的人，你必须意识到，很有可能你永远无法确认这些怀疑是否有事实根据。

或者，你关注的方向可能错了：也许实际上的问题出在团队里的另一个人身上（此人可能通过散布谣言来掩盖自己的行踪）；再或者，问题可能源于团队成员对安全的疏忽大意，又或者某些成员正遭受技术性监控，且其本人尚未察觉 ……

[image]

在这些情况下，最好暂时放下怀疑。你可以从其他角度审视问题：

考虑你的团体或集会目前正在做什么，

朝那个战略目标方向发展的 风险是什么 ，

或者，泄密是否会导致你们无法继续使用选定的方法开展政治活动。

我们建议，处理此问题的良策是增强安全意识并采取一切可能的预防措施；就政治项目可能面临的威胁以及应对措施进行公开的、坦诚的辩论。

[image]

返回训练题板块：💯训练-SelfDirectedTraining

在许多情况下，你永远无法 100% 确定某人是渗透者。这会让你陷入“下一步该怎么办”的痛苦抉择。例如，在英国关于卧底警察的公开调查背景下，“卧底研究小组”（Undercover Research Group）等组织公布了一些渗透者的信息，尽管没有确凿证据，但他们认为已有足够的迹象予以证实。在这些案例中，由于仍存在微小疑虑，他们限制了发布的信息内容：决定不公开照片和全名。

在西班牙也有类似案例，但他们目前的决定是在获得“确凿证据”前不

公布任何信息。玛丽安（Marian）就是一个例子，她于 2021 年被“母亲反压迫”组织开除，但直到 2024 年才通过证据100%证实了其真实身份。

3. 如果你是对的……

如果你找到了确凿证据，或者重要到无法忽视的间接证据，你需要仔细考虑下一步行动。

公开消息几乎总是一个好主意，因为大多数渗透者的活跃程度往往超出我们的想象，可能涉及更多地区和运动，而不仅仅是你所在的团体。所有可能受到影响的群体都应知晓此事。

公开信息需要格外小心。可以遵循以下步骤：

- 预先告知： 尽力提前通知那些与渗透者有过接触的人。虽然并不总是能做到，但在这一方向上做出努力非常重要。通过互联网或新闻看到照片才知道自己以前的同事、搭档或朋友是卧底警察，那种感觉会非常糟糕的。

- 保护匿名性： 明确哪些人的匿名权需要保护，并确保认识渗透者的每个人都意识到，未经许可不得透露任何个人细节，例如相关人员的真实姓名（这对于与渗透者有任何形式亲密关系的人尤为重要）。

- 准备证据链： 整理所有证据。如果可以，与可靠的独立媒体合作发布，以获得传播覆盖面。确保联系那些理解你们的需求、理解此类事件对人产生的心理冲击的记者，特别是对那些与渗透者有过亲密关系的人来说。这包括时间安排、发布内容等方面的管理。此外，最好尽可能详细地提供渗透者参与活动的细节以及他们进入后的整个履历，以便其他团体和个人进行背景比对：人们对名字和面孔的记忆可能比较模糊。通过这种方式，可以帮助他人了解正在谈论的对象，并识别与其他尚未调查案件的共同点。

- 内部管理： 小组内部对这一过程的管理至关重要。必须为那些受后果影响最深的人准备好支持。根据我们的经验，获得专门从事政治暴力、虐待和酷刑受害者关怀中心（如 Sira）的支持是必不可少的。

- 类似“我早知道”这类反应应该尽力制止： 这类反应毫无帮助，尤其是对受影响的人来说。请记住，受害者可能仍在与愧疚感、自我厌恶等情绪作斗争，这些问题可能需要数年才能化解。更重要的是，这种反应反映的是恐惧、不安全感和不接纳。很明显，如果这些人真的“早知道了”却什么也没说、没做，那他们根本谈不上是在支持同志。

[image]

经验教训和后果

如果你发现身边潜伏着渗透者，该怎么办？

通常情况下，你应该保持谨慎。因为在这种境况下，不仅存在散布偏执情绪的风险，还存在当事人察觉到被怀疑的风险。一旦发生这种情况，他们极有可能会掩盖行踪，在你有机会跟他们对质之前就消失得无影无踪。

本手册讨论的九个案例中，大多数是渗透者“撤离”行动的过程中被发现的。当时他们已不再居住在渗透目标的城市，但总会留着回来的余地，通过短信和电话保持着虚拟联系。

[image]

请记住，任何调查 —— 无论结果如何 —— 都可能损害团体内部的信任网络。特别是在公开曝光之后，如果一些人感到自己被排除在调查过程之外，或者因为没机会参与决策而感到愤怒，这可能会成为一个问题。

调查结束后（再次强调，100%的确定性并不总是能达到的），您所在的团体可能需要付出巨大努力来恢复成员间的信任。

刚刚被暴露的渗透者在逃离现场时可能会造成严重的个人伤害。如果我们在调查时没有准备好证据来解释原因，如此重大的发现可能导致群体分裂。如果我们能拿出手的证据不充分，渗透者还可能尝试煽动运动中的其他人或组织来对抗调查方，或者利用逃脱的过程制造摩擦和内斗。

相互支持

调查并揭露渗透者会产生深远的情绪影响。正如国家暴力机器会为专门用来渗透活动的条子提供心理支持，我们自己也应该意识到调查本身意味着什么。

在过程的各个阶段，你必须确保考虑到受影响的所有人、以及调查人员的情绪需求 —— 尽管在我们的案例中，这两者往往是同一群人。

调查阶段提供情绪支持的经验教训

在调查渗透者的过程中，对自己的信心以及对他人的感知能力往往是最先丧失的东西。进行调查对个人造成的冲击常被低估。

团结互助：

通过内部团结，我们可以创造空间，通过分享经验和政治理念以“看到”彼此，从而支持彼此。这是我们最大的力量之一。

重要的是要意识到每个人的反应都不同，这取决于每个人当时的生活阶段以及他们与渗透者的关系。

给予心理缓冲：

与渗透者关系非常亲密的人往往难以接受这种欺骗，理解所发生的一切可能需要很长时间。

在调查期间，必须记住这一点，并当面提供信息和证据，帮助人们消化这些难过的东西。

切勿匆忙决策：

人们需要感到自己的需求得到了重视，因此必须有空间让他们表达。

摒弃前嫌：

尽量抛弃那些可能分散注意力或影响调查客观性的旧有私人和政治恩怨。

尊重选择：

每个人处理情况的方式不同，尊重每个人的意愿和偏好非常重要。有些人宁愿一无所知，有些人可能已经因为生活中的琐事而精疲力竭，无力应对。

调查结束后向集体展示结果时，那些没有被邀请加入调查组的人可能会产生不安。如果管理不当，这可能会是一个棘手的问题。

偏执倾向

意识到自己曾与卧底警察共享空间、共同参与集会、组织、甚至一起生活，可能会引发强烈的恐惧和偏执。常见的症状包括：草木皆兵，觉得每个角落都有间谍，或者指责任何有过轻微可疑行为的人“是间谍”。这是我们必须警惕的。很多因素都会影响我们，但重要的是不

要被恐惧牵着鼻子走，要努力进行严肃的调查。偏执毫无益处，只会破坏调查进程。

如果你正在与那些心存怀疑甚至产生偏执的人共处，重要的是让他们感到自己被倾听和理解。委婉地询问他们的信念或恐惧；真诚但谨慎地倾听他们；以尊重的态度挑战分歧，并保持开放的心态 —— 意识到这可能不是偏执，而是严重的忧虑。

[image]

偏执的另一个侧面是它会伪装成“安全意识”。

区别 —— 安全是为了将风险降低到可接受的水平，以便我们能继续做事；而偏执则只会导致局面失控并阻碍我们采取任何行动，它源于对看似无坚不摧的国家和警力的普遍恐惧。

我们提出的问题有助于通过切实的调查和陪伴来缓解部分偏执。问问自己：我们现在知道什么、我们害怕的是什么，并专注于真实的数据。这通常有助于在客观信息的基础上揭露渗透者，而不是沉溺于恐惧。我们的目的始终都是降低风险，以便继续开展政治活动。

[image]

关键在于分析你的团体或集会是什么类型的，你希望它是开放还是封闭，你的目标是什么，并在此分析基础上建立适配的安全协议，让大家在其中都能感到舒适。

BACK [image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

结语

一次成功的调查虽然揭露了令人不快的事实，却也能因此提振士气、并赋予团队力量。本手册中的材料汇总自多个此类调查过程及其参与者的体验。事实证明，经历这些案件的团队完全可以在此之后变得更

加强大，尽管我们走过（并仍在走）的道路往往崎岖不平。

编写这份文件的初衷并非鼓励偏执，恰恰相反，是为了减少偏执。指责往往基于谣言和臆测，这只会导致亲痛仇快。我们尝试提供一些工具和技术，帮助您在自己的团队中进行深入调查，终结谣言和错误做法，并在此过程中强化自身。

尽管警察和国家对有组织的工人阶级发动了猛烈进攻并造成了深重伤害，但他们 并没有 能摧毁我们。陷入“无能为力”的宿命论只会让敌人得逞。我们仍有许多可为之事，有许多值得为之奋斗的远景，也有许多战役等待打响。

随着我们找到解决方案，战术会改变、会调整、会适应现实环境，但最重要的是最初驱使我们投入政治斗争的动力，以及我们所追求的解放目标。

经验显示，渗透者的使用有时也会产生意想不到的副作用，例如引发诉讼、甚至间接协助了某些行动。我们知道有些案例中，卧底警察的存在反而保护了激进分子 —— 要么是因为担心暴露渗透者的身份而不敢根据某些情报采取行动，要么因渗透者以“激进分子”假身份卷入法庭案件而无法行动。

最后，一个经常被问到的问题是：抓特务的风雨散去后，我们如何重新吸引新成员加入我们的组织？如何平衡开放性与安全性？正如之前所说，没有唯一的标准答案。每个集体都有自己的需求和优先级。重要的是从一开始就建立一种符合组织抱负并能坚持下去的文化。不要害怕提问，但要诚实地说明提问的原因。 如果你认为需要更高水平的安全或保密措施，请弄清楚你面临的具体威胁是什么，并计划如何应对以最小化风险。世界上没有 100% 的安全，但总有寻找解决方案的方法。

[image]

返回训练题：[image]S01E01-T2 识别威胁并作出反应

国家暴力机器可能会投入巨资试图阻止我们，但成千上万的行动已经

开展，许多组织正采取预防措施并成功运作，这清楚地证明了：只要我们严肃对待，我们就能比他们更聪明。

[image]

研究材料

案件资源

在开始本节之前，我们想强调的第一点是：阅读媒体发布的关于已曝光案例的每篇文章都至关重要。正是通过阅读首批披露的文章，我们才发现了其中的共同模式，并发现许多特征与嫌疑人吻合。

为了集中这些信息，以下列出的是直接跳转至相关报道的链接（西班牙语和加泰罗尼亚语）：

- Carlos Pérez Moreno: elsaltodiario.com/policia/policia-infiltrado-movimientos-sociales-madrid-juancar

- María Ángeles Gómez Armendáriz: elsaltodiario.com/policia/marta-estupa-dos-decadas-infiltrada-movimientos-sociales

- Ignacio José Enseñat Guerra: directa.cat/un-agent-de-la-policia-espanyola-sinfiltra-a-lesquerra-independentista-i-al-moviment-pel-dret-a-lhabitatge

- Daniel Hermoso Pérez: directa.cat/dani-el-segon-talp-destat-per-espiar-lactivisme

- María Victoria Canillas Sánchez: elsaltodiario.com/policia/identifican-una-agente-policia-infiltrada-movimientos-sociales-madrid

- Ramón Muñoz Fernández: directa.cat/un-talp-policial-en-lactivisme-de-valencia

- Sergio Gigirey Amado: elsaltodiario.com/policia/seis-anos-infiltrado-movimientos-sociales-madrilenos

- Lucía Rodríguez de Ves: eldiario.es/politica/policia-espio-colectivos-sociales-madrilenos-durante-tres-anos-agente-infiltrada_1_11312665.html

- María Isern Torres: directa.cat/una-policia-sinfiltra-tres-anys-en-els-moviments-populars-de-girona

调查工作中最常使用到的关键问题

1. 此人是否没有生活背景？缺乏社会根基？

通常，渗透者的背景非常单薄。他们往往有一套“说辞”：来自哪里，为什么离开。细节通常很模糊，且他们过去的世界与现在的抗争世界几乎没有重叠。

你很难见到他们的旧友，或看到他们“以前”生活的照片，即使他们口头上可能经常提起，或声称要去会面老朋友。

由于这些身份是为了渗透而伪造的，他们没有“过去”，你在任何记录或互联网上都查不到相关痕迹（除非是渗透工作开始之后的记录，如报名的体育赛事或大学注册信息）。

在绝大多数案例中，渗透者的原籍城市与开展渗透工作的城市不是同一个，我们推测这是为了防止被认出，或防止过去的经历被轻易核实。

注意： 在赫罗纳（Girona）案中，已证实玛丽亚向活动家介绍了自己真实的家人和朋友（非公职人员）。这被认为是为了增强故事可信度。因此，调查时记住这些人的细节和地址非常重要。

2. 此人的政治观点是否很模糊、或者不够成熟？

这点至关重要。

大多数渗透者对其渗透的运动的政治理念根本不怎么明白，所以他们极少在这方面发表见解。虽然他们表现出很大的倾听兴趣，但贡献却极少，他们只会鼓掌、模仿、迎合，通常会避开或远离深度的辩论。另方面，在后勤、财务、出席会议和行动等方面，他们往往是“模范积极分子”。

请注意，这里指的是对具体的政治运动和项目而言。而不是以“抱团取暖”为唯一目的的普通异议圈子。在后者情况中，对镇压/压迫的感知是最主要的凝聚力，而非抵抗战略理论和路线层面的共识，于是其中可能不乏政治模糊的状况。这需要针对性分析。

不论如何必须说，如果一个人并不真正理解为什么应该抵抗，不理解苦难的根本性原因，那么此人在抵抗圈子中的存在至少是不恰当的。

3. 有没有人见过此人的家人？

有些人从不谈论家人，有些人则说得特么多，但你永远都见不着他们提到的人，总有借口回避掉。有些人会利用病重的父母作为长期离开的借口。

例外： 在赫罗纳案中，渗透者不仅介绍了真实的家人，其母亲甚至在整个行动中通过视频电话扮演了积极的角色。

强调：此项与社会/社群文化有关，不可完全照搬，应结合其他问题加以分析。

4. 工作或“个人”生活是否导致此人长期或频繁短期失踪？

许多卧底的“工作”会迫使他们离开数周（通常在夏天）。这些缺席的时段往往还伴随着金钱的解释（例如：回家后带回一笔钱，声称是长辈给的，从而解释为何一段时期内不用上班）。

如果你们是在同一个项目中，或者至少是一个紧密合作的社群，这一指标可能很重要。但如果你们只是一个朋友圈子，日常相处更多属于情绪价值交换，此处则不一定适用。

5. 此人的住处是否看起来冷冰冰的缺少人气？

一个共同点是，他们的家显得冷冰冰的，没有生活气息。屋内可能摆放了一些刻意布置的“政治书籍或材料”来标榜身份，但那不意味着任何事。

比如渗透者卡洛斯的家几乎没有装饰，水龙头出来的水甚至是褐色的；玛丽亚则在旅游公寓“住”了三年，一张装饰画都没换过。此外，这些人获得住房的方式往往带有些“运气成分”（比如：借叔叔的房子住、母亲朋友的房子等等）。

6. 他们是如何进入组织或社交圈的？

渗透者通常从开放的、政治色彩较淡的活动切入：比如食品银行、社区健身房、女权主义读书会等等。这为他们进入更具政治性的空间提供了“背书”。

并不是说这一路径本身“不正常”（说实话比那些靠攒粉丝量出名然后割韭菜的网红大佬们“正常”多了）。相反可以说这是一种常见路径。也正因此，此条结合上述第2条是重要的 —— 基于政治立场的参与者始终会把精力集中在政治理念方面；带任务的渗透者则将精力集中在拉帮结派搞人际方面。

7. 是否有超凡的驾驶技术或持有多种驾驶执照？

许多渗透者的驾驶技术高于常人，这与国家警察的入职要求有关。比如在英国，渗透者通常都是老练的警官；在西班牙，虽然多是刚毕业的警察被安排做渗透，但至少都持有驾照（入职考要求）。

在您那里的警察学校都有哪些课程和考核标准？这些都是作为激进社群值得了解的。

8. 他们的态度或性格如何？

渗透者通常表现得非常有魅力、友好且乐于助人。他们看起来八面玲珑，避开任何争议，并表现出极强的同理心和精明，擅长处理他人的情感危机，以此作为情感支撑，但又会小心地不侵犯隐私。

并不是说人缘好的人都“有问题”。有的人的确有天然的魅力/感召力，这是性格所致，关键要看此人如何使用这一能力 —— 推动运动项目，还是操纵他人、把玩人脉。

9. 钱方面是否不明不白？

这类人通常表现得很慷慨，愿意替人付油钱或请客吃喝。他们不一定显摆，甚至会抱怨财务状况以求合群，但实际上似乎总能随时动用资金。

10. 社交关系是否集中在核心人物身上？

进入圈子后，渗透者往往很快“锁定”圈子核心人物，并千方百计与之建立亲密关系。这不仅能获取情报，还能通过成为“某人的左右手”来消除外界怀疑。

有攀爬文化、崇尚等级地位的团体是很危险的，因为多数人会被激励

着这样去做，在这种环境中真正的渗透者将很容易隐藏自己。

11. 是否检测到任何怪异或矛盾之处？

- 证件姓名不符： 偶尔被发现此人持有不同名字的证件。

- 真实的社交网络： 渗透者玛丽亚的暴露部分源于此。她提到的学校名称与实际不符，通过社交网络发现了她的真实姓氏，与其伪装姓氏不同。

- 缺乏应有的技能： 比如声称对某事感兴趣，却毫无常识，或声称从未练过武术却在第一节课上表现得像个老手。

- 对意外状况的反应： 面对突发状况时展现出受过训练的反应。已证实渗透者背后有团队全天候监控，通过其电子设备（手表、手机、电脑等）的麦克风进行监听。曾出现过这样的情况：当渗透者及其团队所在区域出现大量噪音时，由于无法掌握现场状况，他们会通知最近的巡逻队以"例行检查"为借口前来查看，以免引起怀疑。此外，多起案例证实：潜伏者居住的楼栋内的部分公寓实际上全住着警察；即便没有警察住在那里，附近也肯定有国家警察分局。

- 面对信息失控或突发状况的不确定性 —— 诸如临时变更、即兴计划等 —— 表现出过度且隐蔽的焦虑。也许这种失控带来的紧张感不难理解，但在调查过程中或许值得留意这一细节。

12. 是否出现过离奇的诉讼撤销或警察缺乏兴趣的情况？

有时卧底会莫名其妙地从诉讼名单中消失，或者在明显的违法行动中，警察却反常地没有实施逮捕，这是为了避免暴露卧底的身份。

警告：有些时候情况可能会恰恰相反！

13. 是否突然消失并切断所有联系？（脱离/撤离）

这个问题本身可以单独成章，因为"撤离策略"或"撤离行动"是调查警方渗透行为的重要环节之一。在所有已知案例中，卧底人员通常会持续执行"任务"数年（部分因暴露而提前撤离；另一些则更持久，长达七年），随后往往突然撤离（借口换工作、亲属重病等等）。

提醒注意，“换工作”和“家人重病”这两种策略被反复运用，有时还会结合使用。尤其后者，扮演良善以博得同情，更成为逐步撤离的借口。

撤离即切断现实社交渠道。但通常会保留虚假身份的社交账号或电话，维持一种“若即若离”的线上联系，以便日后需要时能随时返回。

在此，有两个非常关键的问题需要您在处理过程中重点关注：

A、接力和行动：

我们发现多起案例中存在渗透者之间的接力行动。例如，卡洛斯和露西娅接替了塞尔吉奥离开后在两个组织中的职位。另据情报显示，其他案例中也存在一个“前人”渗透者为新人渗透者铺路的现象，但目前尚无法透露具体细节。

关于人员流动，您需要特别注意的是：即使某人已经因嫌疑而遭驱逐，但只要尚未公开处理，他们就仍然可以转移活动。典型案例包括卡洛斯因其渗透的青年团体解散而转战巴列卡斯区，以及伊格纳西奥·何塞和拉蒙同时活跃于多个组织和场合的现象。

B、一旦身份暴露后的反应：

尽管这似乎显而易见，但所有被发现的卧底人员都会强力否认便衣身份。无论是面对发布报道前联系他们的媒体，还是在各种场合接触过的"同事"和"朋友"，他们都矢口否认。即便面对身着警服的照片或视频等确凿证据，他们依然坚持否认。

我们推测这是警方的惯例操作，但此举反而造成了更大的损害 —— 如果这还可能的话。唯一例外是玛丽亚的案例。她在视频通话中承认自己是警察，并解释了警局如何在她宣誓就职后联系她担任卧底，还坦承马拉加、萨拉曼卡和格拉纳达等城市还有更多警察在执行卧底任务。

14. 社交网络

我们发现的另一种常见模式是：渗透者通常在开始渗透行动前不久才创建了专门用于假身份的社交网络账号。调查嫌疑人时，社交媒体部分至关重要。除了查看账号创建时间外，还需要留意其关注者/好友构成 —— 因为极少有人仅关注刚认识的人而完全没有过往人脉（这与问题1中提及的缺乏根基现象相呼应）。在Instagram上甚至能查看到用户名变更次数。

当然，如同所有普遍模式，一个人可能存在充分的私人理由这样做：比如从未建立社交网络而临时创建新账号，或者因为想要与过去决裂而断绝旧交…… 但这一细节仍是值得注意的事实。

15. 照片

他们通常极力避免出现在合影中，并找各种借口不分享自己过去的照片。讽刺的是，与此同时他们常以“开玩笑”或“做表情包”为由拍摄大量其他成员的照片。

此外，不同渗透者之间会共用照片作为互相的“背景证明”（例如：丹尼和伊格纳西奥在伪造身份中被设定为兄弟）。

强调：此条针对激进项目团体而言，在这种情况下合影具有高风险，某些时候甚至意味着誓言。相反自由派饭局圈子的合影则意味着晒人脉资产，作为背书或交易。拒绝参与后者的合影理所当然。

……

重要数据特征

- 姓名关联： 渗透者的真实身份与虚假身份通常使用相同的名字（除了 Ignacio José 伪造为 Marc，以及 María Ángeles/Marian 伪造为 Marta 之外）。他们往往倾向于使用双姓（例如：真名叫 Sergio，假身份叫 Sergio Manuel；真名叫 Lucía，假身份叫 María Lucía；真名叫 Carlos，假身份叫 Juan Carlos 等等）。这可能是为了防止被打招呼时反应不流畅。

- 极其重要： 他们的真实身份与虚假身份拥有相同的出生日期。

- 官方记录： 他们的真实姓名会出现在《国家官方公报》（BOE）中。在 2022 年之前，其真实姓名也会出现在国民身份证（DNI）上。由于数据保护法，公报中不会包含完整的 DNI 号码，这使调查增加了一定难度。

- 渗透时机： 他们通常在警察学校毕业几个月后开始启动渗透工作。因此，应重点查阅当年的《国家官方公报》（例如：塞尔吉奥2014年5月毕业，同年7月就出现在了莫拉达腊区）。

- 学院经历： 他们会在阿维拉警察学院接受一年左右的培训。在根据嫌疑人年龄判断其是否可疑时，这一事实必须纳入考量。

- 社交网络： 辅助虚假身份的社交账号几乎是在渗透开始的同时创建的。

- 影像资料： 毕业典礼或离开警察学校后的实习工作中的视频和照片（发布在 YouTube 或网络新闻中），通常是曝光卧底的好办法。塞尔吉奥就是这样被抓到的。

- 交叉验证： 对比真假身份的一种近乎决定性的方法是，通过有数据查询权限的可靠渠道（例如医护人员）核实虚假身份与真实身份的出生日期是否一致。

- 房产查询： 查明房屋或店面的所有者。实际应用： 如果你怀疑某人并知道其地址，可以想办法获取该公寓的产权证明，查看业主是谁，对照被调查者告诉你的“故事”是否与此一致。

- 学业情况： 在已曝光的案例中，已证实部分渗透者使用虚假身份报读大学；同时至少有两人（塞尔吉奥和露西娅）在卧底期间使用真实身份报名（在塞尔吉奥的案例中是为了参加内部督察考试）。另一个例子是卡洛斯和丹尼，两人都声称学过空调维修的职业培训课。

- 加引号搜索身份证号（或其他数据）： 在搜索引擎中输入带引号的真/假身份证号，结果会显示该特定信息出现的所有位置。例如，通过这种搜索，我们发现塞尔吉奥在渗透期间获得了国立远程教育大学（UNED）的法律学位。

- 所在地证明： 这是由土地登记处出具的告知性文件，列出了该人在哪些登记处拥有房产权利。由此可以查出渗透者拥有的房产、及其真实身份下的家庭住址，因为他们的姓名和身份证号通过公报是公开的。

- 车辆所有权查询： 这是一个可以在线完成的程序，只需车牌号。例如在玛丽安的案例中，通过记录其曾使用的车牌并查询所有权，最终证实了其真实身份。

- 影像鉴定专家： 专家可以比对渗透者的真实生活照片与虚假生活照片，判定是否为同一人。

- 真实身份的社交网络： 令人惊讶的是（可能是出于一种肆无忌惮的优越感），许多渗透者及其提到的亲友往往在主流社交媒体平台（Twitter、Instagram、Facebook等）拥有真实身份的账号。

以上所有数据都有助于建立调查的起点。如果您知道他们开始渗透的具体日期，并考虑到他们几乎总是使用相同的名字，就可以在相应的

公报中进行初筛。

如果知道嫌疑人的出生日期，可以通过信任渠道进行比对。如果知道具体住址，可以通过产权查询来验证其说辞。如果他们声称在某地工作，可以尽可能隐蔽地去核实。

在 YouTube 和互联网上，有很多警察宣誓就职和在不同城市开始实习的视频或照片。虽然近年来扩招规模巨大（2000-3000 人），但仍有可能像塞尔吉奥案那样准确定位。那些高傲自大认为自己可以逍遥法外而保留真实身份社交账号的渗透者，总会留下痕迹。在卡洛斯案中，一个关键的确认点就是通过他关注了家乡政府的账号而锁定了他的 Instagram 真实身份主页的。

简而言之，只要掌握了渗透者虚假身份的细微信息，就有许多线索可循。如果能在新人正式加入队伍之前的预备阶段获取这些信息（姓名、电话、学习/工作地点、原籍、地址、亲属等等）能极大地方便未来的调查。尽管，必需说，结识新人的初衷应该是社交，而非单纯为了安全。

[image]

返回：[image]结识新认识的人时您应该曝光自己多少信息？- 原则和技巧

成员加入组织前的可行（/但非万能的）筛选机制

如前所述，没有百分百的安全。各组织应根据自身需求进行评估。

以下是基于我们自己的经验的建议：

1. 要求提供工作经历： 且不给其准备时间（最好是类似短信验证的快捷）。

1. 要求提供出生证明： 在西班牙的案例中，我们核实到民事登记处对他们出生证明请求的回复是否定的——也就是说：他们不存在，没有出生记录。这与英国的情况大不相同，英国渗透者的虚假身份通常窃取自夭折的婴儿。

   - 情况一： 被调查者并不知情，调查组利用其基本信息（姓名、身份证号）去申请查询。

   - 情况二： 作为预防手段，要求新成员在其他成员陪同下当场申请。但联系方式（如接收证明的邮箱或地址）必须是组织控制的。

1. 任何官方文件： 任何你认为可以瞒着被调查者获取到的、或者虽然他们知情但你能掌控时间差的官方文件。

是否存在“红线”？—— 渗透者不能干什么

迄今披露的案例使我们得以破除那些那些关于卧底警察“行为准则”的迷思或禁忌。

我们深知，许多人曾坚信卧底人员“遵循特定行为准则，存在不可触碰的红线”。我们指出其中部分案例，正是为了认清渗透者的行动/行为边界，以免掉以轻心。

过去有人认为卧底警察永远不会：

- 参与“非法”行为。

- 与目标对象发生性关系。

- 拥有带合同的正式工作（在卧底的同时）。

- 同时使用真假身份注册学籍。
- 介绍其真实的家人/朋友给被渗透的组织。
- 动用与警察系统无关的平民来支持其不在场证明。
- 拥有虚假身份下的公共文件（身份证、驾照、社保、银行账户、租房合同等）。
- 将虚构故事的一部分建立在真实生活基础之上（例如真实的母亲或真实的消防员哥哥）。
- 纹很酷的纹身（比如丹尼案和塞尔吉奥案中都有。打破了“警察不能有纹身”的神话）。
- 使用社交软件（热门交友软件）接触目标。
- 在未经允许的情况下搜集同事的生物样本或生物特征证据。
- 由警方伪造公司工资单（被涉及的公司并不知情）以签署租房合同。

事实证明，以上所有行为卧底警察都做过。

结论

如果你遇到某人的故事符合上述某些特征，并不一定意味着他就是渗透者，这只是说明你的怀疑值得进一步调查。本手册是一份指南和起点，而非魔法公式。

虽然我们在西班牙和英国的渗透案件中发现了共同模式，但这不代表没有其他未被证实的模式存在。本手册将随新案例的出现而更新。

历史上，警察渗透一直被视为禁忌话题（出于羞耻感、认为这代表“软弱”等等），导致相关经验无法有效传递，也缺乏管理怀疑和预防渗透的机制。因此，我们再次强调公开案例、共享信息、建立工具的重要性。

我们坚决反对仅凭猜疑就散布谣言，建议尽快进行严肃调查。未经证实的谣言只会对组织造成巨大的内部破坏。同时要记住，渗透者的行为会根据目标和环境而变化，他们身后有一个完整的团队在计算每一个举动的战术功效。

我们也观察到，有很多正当理由会让普通人也符合某些“可疑特征”（例如与家人断绝往来、因疲惫而突然退出等等），我们的框架并非万无一失。每个案例都是独特的。

遗憾的是，在某些案例中遇到了部分曾接触过渗透者的活动家拒绝配合。这种对调查的阻碍往往源于过去的个人恩怨。这需要高度的政治觉悟和远见才能明白何时该放下成见。

最后，我们想指出：虽然出发点是好的，但如果使用“我们组织是和平的/无害的”作为反抗警察渗透的论据，这在战略上是错误的。这会抹杀任何革命潜力。虽然目前这些社会运动对国家不构成直接的威胁，仅从事公民抗命（如阻止驱逐、反法西斯自卫、大罢工等等），但基于所谓“无害性”的辩护是在宣告我们永远无法改变现状。同样，将“法律”作为核心论据也是危险的，因为国家随时可以修改法律使其合法化。重点在于意识到：国家在对抗任何有组织的工人阶级时，是没有任何“红线”的。

这并不代表我们不能在特定时刻利用其违法性开启战线（如在巴塞罗那、赫罗纳和瓦伦西亚提起的诉讼中）。

作为本手册的编撰者，我们希望这份文件能对大家有所帮助。我们将我们自己从所有痛苦经历中习得的教训转化为文字，希望能让您从一

个更高的起点出发，而不必像我们当初那样从零开始。

欢迎提出疑问、建议、更好的是，分享您的切身经验，以不断完善这份手册。

□

By NoTrace

[image]
[image]

宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切

[image]	关键词	伪装 分身 审讯心理学 心理安全 心理操纵 欺骗 洗脑宣传 社交工程
[image]	关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；❤🔥行动安全性-OPSEC ；🍎心理安全-PsychologicalSecurity
[image]	创建时间	2026年4月9日
[image]	**Description**	反渗透和协作；行动安全性；心理安全

中央情报局官方欺骗与诡计手册结构版。

欺骗不是制造虚假现实，而是塑造他人对现实的解释。

- Table of Contents
第一章：欺骗的基本原则
一、欺骗的本质
二、人类认知弱点（欺骗的基础）
1. 期望偏差
2. 注意力有限性
3. 权威与信任机制
4. 认知惰性
三、欺骗的结构模型
欺骗三要素：
四、成功欺骗的原则
1. 简单原则

2. 一致性原则
3. 冗余原则
4. 时间控制
5. 最小暴露原则
五、欺骗和反欺骗
六、历史案例（概念性）
第二章：伪装技术
一、伪装的目标
二、伪装的层级
1. 外观伪装
2. 行为伪装
3. 语言伪装
4. 情境伪装
三、有效伪装的原则
1. 平庸原则
2. 一致性原则（再次强调）
3. 文化适配
四、常见伪装方式（概念总结）
1. 职业伪装
2. 社会角色伪装
3. 权威伪装
五、快速伪装 vs 长期伪装
快速伪装：
长期伪装：
六、伪装中的关键细节
七、反伪装（识别伪装）
1. 不一致检测
2. 细节异常
3. 情境不合理
第三章：隐蔽通信
一、隐蔽通信的基本目标
二、通信模型的重构
三、主要方法类型（分类体系）
1. 显性通信中的隐性信息
2. 双重用途通信
3. 信号触发机制
这类方法的特点：
4. 一次性系统
核心原则：
优点：

缺点：
四、通信安全的核心原则
1. 信息最小化原则
2. 风险分散原则
3. 冗余与校验
4. 行为一致性
五、失败模式分析
1. 模式暴露
2. 复杂性过高
3. 操作明显繁琐
第四章：隐匿与藏匿技术
一、隐匿的基本逻辑
理论基础
二、监视和搜查模型
搜查行为有三要素：
三、隐匿策略分类
1. 可见但不可识别
目标：
原理：
2. 物理层面的不可见
传统隐藏方式：
缺点：
3. 分散存储
4. 动态隐藏
四、环境利用
1. 结构冗余
2. 视觉盲区
3. 功能掩护
五、时间维度的重要性
1. 短期隐藏
2. 长期隐藏
两者策略不同：
六、风险管理原则
1. 单点故障风险
2. 可恢复性
3. 曝露后的影响控制
七、反隐匿（搜查方法）
1. 系统化搜索
2. 异常检测
3. 行为线索

第五章：特工工具和技术装置
一、工具的功能定位
二、工具的功能分类（核心框架）
1. 信息记录工具
关键特征：
2. 信息传递工具
关键变量：
3. 隐匿工具
特点：
4. 操作辅助工具
本质：
三、设计原则（核心理论）
1. 双重用途原则
2. 最小化原则
3. 一致性原则
4. 可否认性原则
四、技术与人的关系
五、失败模式分析
1. 过度依赖技术
2. 技术暴露
3. 使用不当
六、理论
第六章：行动策略与操作方法
一、行动的基本结构
行动四阶段模型：
二、准备阶段
1. 信息收集
2. 行动方案设计
3. 角色构建
三、进入阶段
1. 正常化路径
2. 行为匹配
3. 注意力规避
四、执行阶段
1. 时间压缩
2. 动作最小化
3. 环境适应
五、撤离阶段
1. 行为连续性
2. 痕量控制

3. 时间错位
六、风险管理体系
风险三分类：
七、冗余与备份机制
八、行为伪装
九、失败的根本原因
第七章：特殊操作和综合应用
一、从“技术”到“系统”的跃迁
二、系统构成要素
1. 身份系统
2. 信息系统
3. 技术系统
4. 行动系统
5. 风险系统
三、系统耦合
四、复杂环境下的应对策略
1. 不确定性管理
应对方式包括：
2. 多路径策略
3. 渐进式行动
五、协同与分工
1. 分工原则
2. 协同机制 - 连接单个行动单元
六、典型的失败结构（系统视角）
七、认知层面的整合
第八章：欺骗的哲学和战略
一、欺骗的本质：再定义
二、现实的三层结构
1. 客观层
2. 感知层
3. 解释层
三、信息与权力
四、不对称性
1. 信息不对称
2. 认知不对称
3. 结构不对称
五、最小干预原则
六、长期欺骗 vs 短期欺骗
短期欺骗：
长期欺骗：

七、欺骗的伦理与限制（描述性）

 本手册中使用的导图可在这里下载：https://mega.nz/file/f9YwQTSC#yj-u1MCeiSZQv9odjnLHBmZe3e88lIRB-H0XKTUyFqg

[image]

第一章：欺骗的基本原则

理论基础部分，核心在于回答一个问题：欺骗为什么有效，以及如何设计成功的欺骗行动。

一、欺骗的本质

“欺骗”的定义：

> 有意识地操控他人感知，使其形成错误判断，从而影响其行为。

重点不在“说谎”，而在于：

- 控制信息输入
- 利用人类认知漏洞
- 引导对方“自己得出错误结论”

这意味着最成功的欺骗往往不是直接造假，而是：

- 半真半假

- 利用目标人的既有信念

- 顺势而为

二、人类认知弱点（欺骗的基础）

欺骗并非孤立技巧，而是建立在人类认知机制、社会结构与互动规则之上的综合性现象。

4个关键心理机制。

1. 期望偏差

人们更容易相信：

- 符合已有认知的事物。

- 看起来“合理”的异常。

[image]

结论：好的伪装不是要追求“完美”，而是要致力于“符合预期”。

---

2. 注意力有限性

人类注意力极其有限：

- 同时只能专注少数信息

- 容易被显著刺激吸引

因此：

- 欺骗常通过“转移注意力”得以实现。
- 真正关键的内容往往被隐藏在边缘。

[image]聊天机器人的设计“初衷”就是为了让你产生妄想：这不是漏洞，而是商业模式

---

3. 权威与信任机制

人类天然倾向信任：

- 制服（公家人儿被默认为“靠谱”）
- 标志（开迈巴赫撤离激进行动现场没有警察会拦你，镇压机器默认有钱人不会造反）
- 专业语言（越绕嘴越唬人）

这构成了“社交工程”的核心基础。[image]S08精神心理安全-总章节：唤回心灵

---

4. 认知惰性

有反思意识的人少之又少。绝大多数人一旦形成判断，就不愿修正了。

因此：

- 第一印象极其关键。
- 初始误导可以长期维持。

三、欺骗的结构模型

欺骗三要素：

1. 掩护
    - 提供合理解释
1. 干扰
    - 转移注意力
1. 操控
    - 引导错误判断

这三者通常同时存在。

四、成功欺骗的原则

1. 简单原则

越复杂越容易失败

→ 成功的欺骗通常基于很简单的结构

---

2. 一致性原则

所有细节必须相互支持：

- 外观
- 行为
- 语言

任何不一致都会破坏整体可信度。

---

3. 冗余原则

关键欺骗点需要：

- 多重支持信息。
- 多个“证据来源”。

---

4. 时间控制

欺骗必须：

- 在正确时间出现
- 在正确时间结束

---

5. 最小暴露原则

避免不必要风险：

- 不展示不需要的信息
- 不增加额外的复杂度

五、欺骗和反欺骗

> 欺骗与反欺骗是动态对抗关系。

即：

- 每一种欺骗技术都会产生识别方法；
- 每一种识别方法又会被规避；

这构成了情报领域的“进化循环”。

六、历史案例（概念性）

一些情报历史中的经典思路：

- 利用假情报引导敌方战略判断
- 利用伪装设备误导侦察
- 利用心理预期制造错误判断

重点不在具体操作，而在于：

[image]

欺骗成功的关键永远是“人”，不是技术。

[image]

第二章：伪装技术

这里是具体应用层面 —— 应用心理操作学框架。关于：讨论如何改变外观与身份，使他人误判。

[image]什么是伪装，如何伪装，如何识破 —— 社交工程攻防基础

一、伪装的目标

伪装并不只是“隐藏身份”，而是：

1. 融入环境

1. 避免引起注意

1. 支持特定身份设定

[image]

核心：不是“看不见”，而是“看起来正常”。

二、伪装的层级

伪装分为几个层次。

1. 外观伪装

包括：

- 面部
- 发型
- 服装
- 体态

目的是：战略性塑造第一印象。

---

2. 行为伪装

包括：

- 走路方式
- 手势
- 习惯动作

这是很多失败伪装的关键漏洞。

---

3. 语言伪装

包括：

- 口音
- 用词
- 表达方式

---

4. 情境伪装

即：

- 在正确环境中出现；
- 做符合身份的事情；

这是最容易被忽视但最关键的一层。

[image]

三、有效伪装的原则

1. 平庸原则

最好的伪装是：

- 不引人注意；
- 没有特色 - 即便事后被怀疑，也很难被目击者描述清楚。 BACK
  平民告密

[image]

“显眼的伪装就是失败的伪装”。

---

2. 一致性原则（再次强调）

例如：

- 商人 → 行为要像商人
- 工人 → 姿态要像工人

任何细节不匹配都会暴露。

---

3. 文化适配

伪装必须符合：

- 地域习惯
- 社会规范

四、常见伪装方式（概念总结）

1. 职业伪装

例如：

- 技术人员
- 服务人员
- 运输物流人员

[image]

原理：这些身份“容易进入场所且不受注意”。

---

2. 社会角色伪装

例如：

- 游客
- 学生
- 普通市民

---

3. 权威伪装

利用：

- 制服
- 标志
- 身份象征

极易获得信任。

[image]

五、快速伪装 vs 长期伪装

快速伪装：

- 用于短时间任务
- 重点在于外观

长期伪装：

- 需要完整的身份构建
- 包括背景故事与行为一致性

BACK [image]卧底警察识别手册2025版 ；[image]什么是“秘密行动”？政府间谍会怎么折腾你...

六、伪装中的关键细节

伪装的失败往往来自“细节错误”。

例如：

- 不符合身份的手部特征（伪装工人，却有着白皙修长的双手）
- 不自然的行为模式（伪装常春藤高材生，却在餐后挡着一群人的面剔牙毫不遮挡）
- 与环境不匹配的反应（在女权主义项目中流露出下意识的色情凝视）

七、反伪装（识别伪装）

一些识别思路如下。

1. 不一致检测

观察：

- 外观 vs 行为
- 语言 vs 身份

---

2. 细节异常

例如：

- 习惯动作不匹配
- 使用错误术语

---

3. 情境不合理

- 出现在“不该出现”的地方
- 做“不符合身份”的事

[image] [image]

第三章：隐蔽通信

核心问题：

> 在被监视或受限的环境中，如何安全、隐蔽地传递信息？

其本质属于信息安全和通信理论的交叉领域。

BACK [image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

一、隐蔽通信的基本目标

隐蔽通信不仅是“传递信息”，而是同时满足三重约束：

1. 机密性：

   信息内容不被第三方理解 —— BACK 加密 。

1. 隐蔽性：

   通信行为本身不被察觉 —— 隐写。 BACK [image]一系列隐写工具

1. 可否认性：

   即使被发现，也无法确认真实意图 —— 暗语明文。

这三者之间存在张力：

- 加密增强机密性，但可能降低隐蔽性。
- 隐蔽性越强，信息容量通常越低。

二、通信模型的重构

传统通信模型：

发送者 → 渠道 → 接收者

隐蔽通信模型则增加两个关键变量：

- 观察者/对手
- 噪音 - 作为掩护机制

因此可形式化为：

发送者 → 渠道 (+ 噪音) → 接收者

↑

观察者/对手（试图检测/解码）

[image] [image]

三、主要方法类型（分类体系）

隐蔽通信方法的几大类别。

1. 显性通信中的隐性信息

即：

信息嵌入在“看似正常”的载体中 —— 藏头诗、隐写术……

例如（概念层面）：

- 日常文本中的编码结构
- 图像或物品中的信息嵌入

其核心特点：

- 信息存在于“表层信息之下”
- 对观察者来说“不可见或无意义”

本质：利用信息冗余进行编码。

---

2. 双重用途通信

通信表面具有寻常合理的用途，但同时承载隐藏信息。

例如：

- 正常信件中包含特定模式，只有收件人知道该注意什么。
- 日常对话中嵌入预设含义，只有听者能感知到。

关键机制：

- 依赖共享语境
- 信息对第三方“语义不可见”

---

3. 信号触发机制

通信不依赖内容，而是依赖：

- 时间；
- 行为；
- 位置；

例如：

- 某行为是否发生 —— 当一切按计划进行时，她的卧室窗户上将挂出蓝色窗帘。
- 某物体是否出现 —— 如果街口的灯还亮着，意味着行动取消。

这类方法的特点：

- 信息量极低
- 隐蔽性极高

---

4. 一次性系统

包括：

- 一次性编码规则
- 一次性密钥

核心原则：

> 每次通信的编码体系完全独立。即便一次被识破，也无法复制结论。

优点：

- 极高安全性

缺点：

- 管理复杂（需要在很高的熟练程度、且彼此信誉也足够高的团队中进行）
- 容易因操作失误而失败（变数很大的高风险情况下操作失误的可能性会提升）

四、通信安全的核心原则

1. 信息最小化原则

仅传递必要信息。

→ 降低暴露风险

[image]信息最小化原则

---

2. 风险分散原则

信息被拆分为多个部分

→ 即使部分暴露，也无法还原整体

https://iyouport.substack.com/p/4-4c7?utm_source=publication-search

---

3. 冗余与校验

在不破坏隐蔽性的前提下：

- 引入校验机制
- 防止误读

---

4. 行为一致性

通信行为必须：

- 融入日常活动
- 避免产生异常模式

五、失败模式分析

比较常见的几种失败原因。

1. 模式暴露

重复使用同一方法就会暴露模式。

→ 被统计分析识别

---

2. 复杂性过高

系统过于复杂，以至于执行人都难以熟练完成。

→ 使用者出错概率上升

---

3. 操作明显繁琐

行为不符合“正常人模式”，难以隐藏在环境中。

[image]

第四章：隐匿与藏匿技术

> 关于，如何在常规系统或环境中隐藏信息或物品，使其不被发现？

一、隐匿的基本逻辑

- 隐匿：防止被直接发现或感知，侧重物理和视觉遮蔽；
- 藏匿：防止被推理或追踪，侧重信息和逻辑隐蔽。

隐匿并不仅仅等同于“藏起来”，而是：

> 控制对手的搜查行为，使其无法发现目标。

换句话说：

[image]

隐匿的核心是“反搜查设计”。

理论基础

- 感知限制原理：人类的注意力和感知是有限的，通过利用盲点和惯性可以实现有效隐匿。
- 可推理限制原理：信息藏匿通过打破可推理线索链，阻断追踪路径。

二、监视和搜查模型

搜查行为有三要素：

1. 搜查范围（Where）

1. 搜查方式（How）

1. 搜查动机（Why）

成功的隐匿策略必须针对这三点进行设计。

三、隐匿策略分类

---

1. 可见但不可识别

目标：

- 物体存在于视野中；

- 但不被识别为异常。

原理：

- 融入环境结构

- 利用大众的“视觉习惯”

这是最优策略之一。

---

2. 物理层面的不可见

传统隐藏方式：

- 遮挡
- 掩埋
- 封闭空间

缺点：

- 一旦被发现，立即暴露

---

3. 分散存储

将信息拆分：

- 分布在多个位置；
- 即便单点被查抄也无法恢复整体。

---

4. 动态隐藏

隐藏位置或方式不断变化：

- 时间变化
- 状态变化
- 没有固定模式

以增加搜查难度。

四、环境利用

> 最好的隐藏不是创造新空间，而是利用已有的空间。

包括：

1. 结构冗余

利用建筑或物体的：

- 空腔
- 多层结构

例如：吊顶、双壁橱柜、加密卷……

---

2. 视觉盲区

利用：

- 视角限制
- 光线条件

在行动前的环境侦查中：留意摄像头的位置和移动模式、光线和阴影。

[image]

BACK 周密的行动计划 ；

BACK [image]监视器排查 ；

BACK [image]地形侦查

---

3. 功能掩护

将隐藏与物体功能结合起来：

- 使检查行为“显得不合理”。

例如：豺狼把狙击枪组装成骨折靴，其本人化装成坐轮椅的老人，安检则不会要求脱下靴子。

[image]

五、时间维度的重要性

隐匿不仅是空间问题，也是时间问题。

1. 短期隐藏

- 防止即时的搜查/查抄

2. 长期隐藏

- 抵御系统性的搜查监视

两者策略不同：

- 短期 → 重视简单便捷的隐蔽
- 长期 → 重视结构合理性，不易引起注意

[image]

[image]

BACK [image]假身份

BACK 渗透者

BACK 分身

六、风险管理原则

1. 单点故障风险

- 避免把所有信息集中在一处

---

2. 可恢复性

隐藏方案必须允许：

- 安全取回
- 不暴露其他信息

---

3. 曝露后的影响控制

即使被发现：

- 不能暴露更大的系统

七、反隐匿（搜查方法）

如何发现隐藏物。

1. 系统化搜索

- 分区检查

- 避免遗漏

---

2. 异常检测

寻找：

- 不符合环境逻辑的结构。

---

3. 行为线索

通过人的行为反推隐藏位置。

[image]

第五章：特工工具和技术装置

> 关于：在隐蔽行动中，工具如何被设计和使用，以支持欺骗、通信与隐匿？

其本质可归入特工技术学 —— 即 技术系统如何嵌入行为策略。

特工工具是为支持情报收集、行动执行和隐蔽操作而设计的物理或电子装置，目的是增强操作者能力、降低暴露风险、提高任务成功率。

一、工具的功能定位

> 工具本身不构成优势，只有嵌入正确策略的工具才有意义。

因此，本节的目的不是列举设备，而是分析其功能逻辑。

二、工具的功能分类（核心框架）

可将所有相关装置抽象为四类。

1. 信息记录工具

功能：

- 捕获信息（视觉 / 听觉 / 文本）

关键特征：

- 低可见性
- 快速操作
- 数据完整性

理论意义：

- 扩展人类感知能力。

---

2. 信息传递工具

功能：

- 将信息从A传递到B

关键变量：

- 传输路径
- 信号形式
- 暴露概率

与前述“隐蔽通信”形成技术对应。

---

3. 隐匿工具

功能：

- 存储或隐藏信息/物品

特点：

- 与环境高度融合
- 具有“正常用途外观”

与第四章形成结构呼应。

---

4. 操作辅助工具

功能：

- 支持执行任务（例如进入、离开、观察等）

本质：

- 降低行动成本
- 提高成功概率

[image]

三、设计原则（核心理论）

一套具有普适意义的设计原则：

1. 双重用途原则

工具必须具备：

- 表面合法用途
- 以及，隐含功能

这是避免被怀疑的关键机制。

---

2. 最小化原则

- 越小越不易被发现
- 越简单越不易出错

复杂工具反而降低可靠性。

---

3. 一致性原则

工具必须与：

- 使用者身份
- 行为模式
- 环境条件

保持一致。

---

4. 可否认性原则

即使被发现：

- 也能提供合理解释

- 不直接指向真实用途

四、技术与人的关系

强调：

> 工具不会弥补操作错误。反而会放大错误。

因此，请注意：

- 技术 ≠ 能力
- 技术只是“能力放大器”

五、失败模式分析

1. 过度依赖技术

忽视：

- 情境判断
- 行为自然性

---

2. 技术暴露

工具本身：

- 不符合环境
- 引起注意

---

3. 使用不当

例如：

- 操作复杂导致失误
- 使用时机错误

六、理论

> 工具效能 = 技术性能 × 行为适配度

如果行为适配度为**0**，则整体效能为**0**。

[image]

第六章：行动策略与操作方法

> 关于：如何在现实环境中执行隐蔽行动？

这本书是典型的技战法体系。

一、行动的基本结构

以下是一个标准行动模型。

行动四阶段模型：

1. 准备（Preparation）
1. 进入（Entry）
1. 执行（Execution）
1. 撤离（Exit）

每一阶段都有不同风险结构。

二、准备阶段

准备阶段的核心目标：降低不确定性。

包括：

1. 信息收集

- 环境信息 - [image]地形侦查

- 行为模式 - BACK 警卫、监视器、巡逻
- 潜在风险 - 通过模拟行动勾画风险模型

---

2. 行动方案设计

- 主方案
- 备选方案 BACK 周密的行动计划

---

3. 角色构建

- 身份设定
- 行为逻辑

与第二章“伪装”形成直接联系。

三、进入阶段

关键问题：

如何在不引起注意的情况下进入目标环境？

策略包括：

1. 正常化路径

选择：

- 常规入口
- 合理的时间

走正门，而不是爬窗户。隐藏在人流中，而不是深更半夜出现。

---

2. 行为匹配

进入行为必须：

- 与环境一致
- 无突兀之处

充分融入环境。

---

3. 注意力规避

利用：

- 人群
- 忙碌时段

- 视觉盲区

行动前的勘查分析要充分。

四、执行阶段

这是风险最高的阶段，其核心原则。

1. 时间压缩

- 尽量缩短操作时间

- 降低暴露概率

---

2. 动作最小化

- 减少不必要行为

- 避免复杂操作

---

3. 环境适应

根据环境变化实时调整行为。

五、撤离阶段

常被低估的阶段，但实际上风险极高。

---

1. 行为连续性

撤离必须：

- 看起来像“自然离开”

---

2. 痕量控制

避免：

- 留下异常迹象
- 引发事后调查

BACK 痕量证据鉴定

---

3. 时间错位

将关键行动与观察时间错开。

[image]

六、风险管理体系

风险三分类：

1. 结构性风险

   （计划本身的问题）

1. 操作性风险

   （执行中的错误）

1. 偶然性风险

   （不可控因素）

七、冗余与备份机制

成功行动往往具备：

- 多路径方案

- PlanB

- 紧急退出策略

[image]

本质是提高系统稳健性。

八、行为伪装

> 不仅仅要“看起来像某人”，还要“行为符合该人”
> —— 不要仅仅模仿，要“真正成为”那个人。

包括：

- 微表情
- 反应速度
- 注意力分布

需要大量反复的练习。

九、失败的根本原因

> 大多数失败不是因为技术不足，而是因为行为异常。

具体表现为：

- 紧张
- 过度控制
- 不自然

[image]

第七章：特殊操作和综合应用

关于：

> 在复杂、不确定、高风险的环境中，如何将多种技术和方法组合为一个有机系统？

其核心属于复杂系统中的策略集成。

一、从“技术”到“系统”的跃迁

前述侧重于：

- 单一方法（伪装 / 通信 / 隐匿）
- 单点工具

而本节将指出：

[image]

真实行动从来不是单一技术能实现的，而是“多层系统的协同”。

二、系统构成要素

一个完整行动系统通常包含五个子系统。

1. 身份系统

- 角色设定
- 行为模式
- 社会位置

对应上述“伪装”部分。

---

2. 信息系统

- 信息获取
- 信息传递
- 信息存储

对应第三、四章。

---

3. 技术系统

- 工具与设备
- 支持性资源

对应第五章。

---

4. 行动系统

- 任务执行路径
- 时间安排

对应第六章。

---

5. 风险系统

- 风险识别
- 风险分散
- 应急机制

贯穿全部。

三、系统耦合

关键问题不是“有没有这些系统”，而是：

> 它们是否彼此兼容？

典型失败来自：

- 身份设定与工具不匹配
- 行为模式与环境冲突

- 信息路径与行动节奏不一致

即“跨层不一致性”。

四、复杂环境下的应对策略

1. 不确定性管理

复杂环境的特点是：

- 信息不完全
- 条件动态变化

应对方式包括：

- 保留决策弹性
- 避免刚性计划

---

2. 多路径策略

设计：

- 主路径

- 备用路径
- 紧急退出路径

本质是提高系统稳健性。

---

3. 渐进式行动

避免一次性完成复杂任务。

建议：

- 分阶段推进
- 每一步都可单独成立

五、协同与分工

1. 分工原则

- 每个行动小组/行动单元只掌握局部信息
- 降低整体暴露风险

---

2. 协同机制 - 连接单个行动单元

- 通过有限接口连接
- 控制信息流动

六、典型的失败结构（系统视角）

> 大规模失败通常不是单点错误，而是系统性配置错误。

例如：

- 小错误被放大
- 局部成功导致整体暴露
- 一个环节失败引发连锁反应

七、认知层面的整合

最终，所有系统仍依赖对目标群体认知的控制。

即：

- 系统的设计必须考虑“别人怎么看”
- 成功取决于“是否被理解为正常”

[image]

第八章：欺骗的哲学和战略

> 阐述一种关于认知、现实与行动的哲学框架。

一、欺骗的本质：再定义

> 欺骗不是制造虚假现实，而是塑造他人对现实的解释。

这意味着：

- 现实本身并不需要改变，
- 只需要改变“解释框架”。

二、现实的三层结构

可以抽象为：

1. 客观层

- 物理世界
- 事实存在

---

2. 感知层

- 人如何看到世界

---

3. 解释层

- 人如何理解所见

[image]

欺骗主要作用于：感知层 和 解释层。

三、信息与权力

关键：

控制信息流 ＝ 控制决策能力

因此：

- 欺骗是一种“间接控制”。
- 不改变对方的意志，而是改变其做判断的基础。

他们不会去说服一个激进的年轻人放弃革命，而是把TA装到鱿鱼世界的跑步机上，让TA“亲身体验到”拒绝996等于无法维生的恐惧感。

四、不对称性

欺骗的力量来自于以下三种不对称性。

---

1. 信息不对称

一方掌握更多或更准确的信息。

故意不让你知道，就意味着准备开始骗你了。

资本主义鱿鱼世界把所有人变成了竞争对手，“信息差”作为博弈筹码构成了所有人对所有人的心理战。

---

2. 认知不对称

一方更理解对方的思维方式。

了解得越深刻，越容易实施操控。

掌握监视权力的人对被监视方的思维方式了如指掌，一个在明一个在暗。

---

3. 结构不对称

一方拥有更灵活的行动结构。

结构不对称的核心在于“依赖性差异”：处于优势地位的一方能够控制流程、信息和资源，从而使劣势方在决策或行动上处于被动。例如，在审讯或谈判中，掌握制度规则的一方可以设置议题、限定信息流动，使对方无法完全理解或掌握全局，从而在心理上产生压力和不确定感。

[image] [image] [image]

五、最小干预原则

高水平欺骗具有一个特征：

[image]

用最小的干预产生最大认知偏差。

为了最大化效果，同时降低抵触和反抗，操控者应尽量减少直接的干预，而是通过微妙的、精准的行动引导目标行为和认知变化。这一原则强调效率、隐蔽性和可持续性，与直接施压或强制性干预形成鲜明对比。

表现为：

- 微小线索 → 巨大误判

- 局部改变 → 全局推论

[image] 关于最小干预原则 - 结构版。

以下是拆分版。

[image] [image] [image] [image] [image]

六、长期欺骗 vs 短期欺骗

短期欺骗和长期欺骗的核心差异：

- 时间维度（即时 vs 延迟）
- 目标深度（表层反应 vs 结构性改变）
- 风险暴露（高暴露 vs 低暴露）

短期欺骗：

短期欺骗指的是为实现即时目标而设计的欺骗行为，其特点是快速、直接、目的明确。例如在审讯中通过虚假信息、诱导性陈述或情境设定，促使目标在短时间内做出反应（如承认、透露信息等）。

- 目标明确
- 风险集中

[image]

长期欺骗：

长期欺骗是一种持续性的策略，旨在通过时间积累建立信任、塑造认知或重构关系，从而在未来某一关键节点实现更深层次的控制或信息获取。这类欺骗往往隐蔽性更强，不以即时结果为导向。

- 需要持续的一致性
- 风险分散，但会不断累积

[image]

七、欺骗的伦理与限制（描述性）

需注意的是：

- 欺骗具有反噬风险
- 过度依赖会削弱系统稳定性

欺骗是一种高风险、高收益的工具，其使用必须受到严格约束。缺乏伦理和制度边界的欺骗，不仅可能损害目标，也会反噬操控者自身，破坏长期目标的实现。真正有效的策略不是无限制地使用欺骗，而是在明确边界的前提下，将其作为有限且可控的手段。

[image]

[image]
https://z-lib.sk/book/2dqRJAGYqY/the-official-cia-manual-of-trickery-and-deception.html

□

[image]
🇨🇳

中国跨境数字镇压的工业化和私营承包商演变：公民实验室最新报告“Tall Tales”

[image] 关键词	个人 人际安全 伪装 团队 新自由主义式跨境镇压 社交工程 诱导 跨国镇压 防御
[image] 关联	[image]宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切 ；[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病 ；[image]什么是伪装，如何伪装，如何识破 —— 社交工程攻防基础 ；[image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术” ；👄套话：5种有效的社交工程启发术 ；[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御 ；[image]了解追踪者的手段和你的弱点：完美隐身 S04E02
[image] 创建时间	2026年4月29日
[image] **Description**	技术直觉；反渗透和协作

对于可能受影响群体，请务必关注本文嵌入标识框中的相关攻击解析和防御建议。

- Table of Contents

一、概述和核心背景

1.1 基本信息
1.2 什么是数字跨境镇压（DTR）？
1.3 宏观政治环境：“五毒”与总体“国家安全”观
1.4 核心研究问题
二、核心机制：伪装身份和叙事劫持
2.1 “伪装身份”
定义
攻击者伪装成有公信力的身份主体，比如：
其目标是：
运作方式
（1）伪造媒体或官方新闻来源
（2）冒充社区内部成员
（3）冒充受害者本人
2.2 “叙事劫持”
定义
主要表现形式
（1）复制真实议题
（2）语境扭曲
（3）制造“内部冲突”
2.3 冒充 + 叙事劫持的组合效应
三、攻击目标和对象结构
3.1 主要目标群体
3.2 攻击目标的选择逻辑
（1）高影响力节点
（2）网络中介节点
（3）弱防御个体
四、技术与策略维度
4.1 社交工程学的核心地位
4.2 与传统网络攻击的区别
报告认为此类攻击的未来趋势包括：
五、影响机制：心理、社会和政治层面
5.1 心理影响
5.2 社群层面影响
5.3 对家庭施压
5.4 政治影响
六、两大攻击行为体深度剖析
6.1 GLITTER CARP：规模化的“初始准入者”
A. 行为特征与目标
B. 攻击技术细节：身份伪装的艺术
6.2 SEQUIN CARP：精准的“社交工程操盘手”

A. 行为特征和目标
B. 核心战术：叙事劫持和 OAuth 滥用
七、跨境镇压的“工业化”和私营承包商生态
7.1 军民融合战略下的激励机制
7.2 低成本和高效率的“黑客超市”
八、攻击行为对社会的毁灭性影响
8.1 破坏社区信任
8.2 寒蝉效应和自我审查
8.3 对新闻自由的侵蚀
8.4 数字威权主义的新阶段
从“监控”到“操控”
从“信息控制”到“叙事战争”
从“国家行为”到“生态系统”
8.5 揭开跨国镇压体系
九、防御建议和政策应对
9.1 针对高风险个人的建议
9.2 针对技术平台的建议
9.3 针对政府的政策建议
十：综合评估和局限性
10.1 报告的核心贡献
10.2 方法论价值
10.3 局限性
（1）归因困难
（2）样本偏差
（3）技术细节有限
最后：一种“软性压制”的全球扩展

BACK [image]宣传、审讯、渗透、操纵、诱导、伪装……关于欺骗和诡计您应该知道的一切

BACK [image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

[image]

“数字跨国镇压” 指的是：国家行为体利用数字技术，将其控制与压制行为延伸至境外，对流亡者、异见者、记者、及少数群体进行针对性的监控、骚扰或威慑。

其关键特征包括：

- 跨境性：突破主权边界；
- 数字化：依赖互联网和信息系统；
- 日常化：成为“常态统治工具”；
- 隐蔽性：较少直接的暴力，更依赖心理操纵和信息操控以实现影响。

与传统的跨国镇压手段（暗杀、绑架）相比，“数字跨国镇压” 成本更低、更难归责、更容易规模化。

[image]

BACK 我们此前解读过一本小册子，其中包含对此等操作手段及其有效性原理的详细描述：[image]宣传、审讯、渗透、操纵、诱导、伪装……关于欺骗和诡计您应该知道的一切

一、概述和核心背景

1.1 基本信息

- 发布机构：多伦多大学蒙克全球事务与公共政策学院公民实验室。
- 发布日期：2026年4月27日。
- 核心议题：揭露与中国政府相关联的行为体如何利用“伪装身

份”和“叙事劫持”手段，对海外异见人士、少数群体及国际媒体，进行数字跨境镇压（DTR）。

- 合作方：国际调查记者同盟（ICIJ）。

1.2 什么是数字跨境镇压（DTR）？

跨境镇压是指国家力量跨越国界，通过物理或数字手段，追踪、骚扰、恐吓和控制海外公民或批评者。数字跨境镇压（DTR）则特指利用恶意软件、钓鱼攻击、社交媒体骚扰、和账户劫持等技术手段，实现的压制行为。

[image]

BACK [image]什么是伪装，如何伪装，如何识破 —— 社交工程攻防基础

BACK [image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

BACK [image]直面你的对手 - 6大原则：完美隐身S04E01

1.3 宏观政治环境：“五毒”与总体“国家安全”观

报告指出，自2012年以来，中国政府在“总体国家安全观”的指导下，加强了对所谓“五毒”（维吾尔人、藏人、法轮功、台湾独立支持者、民主活动人士）的打击。随着习近平主席推动“军民融合”战略，这种镇压行为已从政府部门直接执行转变为“国家资助、私营承包商实施”的高度工业化模式。

1.4 核心研究问题

该报告聚焦一个此前研究较少但高度关键的维度：

> 揭露与中国政府相关联的行为体如何利用“身份冒充”和“叙事劫持”手段，对海外异见人士、少数群体及国际媒体，进行数字跨境镇压（DTR）。

换言，重点不再是技术入侵（如间谍软件等），而是：

- 信息操控 -信息战；
- 认知战 - 诱导和欺诈；
- 身份伪装 - 社交工程；
- 舆论污染 - 掺水裹乱。

这是数字威权治理进入“社交工程＋叙事操控”阶段的重要标志。

[image]

BACK

二、核心机制：伪装身份和叙事劫持

2.1 “伪装身份”

定义

攻击者伪装成有公信力的身份主体，比如：

- 记者
- 学者
- NGO
- 同行活动人士
- 主流媒体机构

其目标是：

- 获取信任
- 引导互动
- 实施进一步的攻击（信息收集、钓鱼、操控）

运作方式

报告揭示了几种典型的模式：

（**1**）伪造媒体或官方新闻来源

攻击者复制真实媒体页面或内容，使目标误以为来自可信新闻机构。

这种策略此前曾在针对华语媒体的攻击中出现，例如仿冒新闻站点进行钓鱼。

（2）冒充社区内部成员

比如：

- 假装成同一运动的参与者
- 假装成志愿者或者组织者

这种方式利用“共同身份”降低防备。

（3）冒充受害者本人

创建假身份账号：

- 复制姓名、头像
- 模仿发言风格

用于混淆信息环境或制造冲突。

2.2 “叙事劫持”

定义

攻击者挪用目标群体自身的话语、议题或价值观，进行再包装和操控。

[image] □ [image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

这比一般意义上的虚假信息更复杂：

> 不是“编造假信息”，而是“操控真实叙事”。

主要表现形式

（1）复制真实议题

例如：

- 人权议题
- 民族压迫叙事
- 政治抗议话语

但加入隐性的操控内容。

（2）语境扭曲

将真实信息：

- 断章取义

- 重新排序
- 重新解释

从而改变其政治含义。

（3）制造“内部冲突”

通过伪装为群体成员：

- 引导争议
- 激化矛盾
- 破坏信任

[image]

BACK [image]卧底警察识别手册2025版

2.3 冒充 + 叙事劫持的组合效应

报告强调，这两种策略往往结合使用：

> 用身份伪装提供“入口”，叙事劫持实现“操控”。

形成完整的攻击链：

1. 建立虚假的且看起来很可信的身份

1. 渗透进入目标网络

1. 引入或操控叙事

1. 扰乱认知、扰乱目标群体的关系结构

三、攻击目标和对象结构

3.1 主要目标群体

报告指出，这类行动主要针对：

- 海外异见人士
- 民主活动人士
- 维吾尔人、藏人等少数群体
- 香港政治活动者
- 独立媒体工作者和记者

这些群体长期处于跨国镇压的重点范围。

3.2 攻击目标的选择逻辑

攻击并非随机，而是具有明确策略。

（1）高影响力节点

如：

- 意见领袖
- 组织者
- 媒体从业者

目标：扩大信息影响面。

（2）网络中介节点

如：

- 社群管理员
- NGO工作人员

目标：渗透整个网络。

这就是为什么担保措施至关重要。尤其是对担保人的担保！

[image]

BACK [image]“我的”朋友还是“我们”的朋友？：如何执行担保措施

（3）弱防御个体

如：

- 新加入的成员（这就是为什么入门安全培训至关重要）
- 技术安全意识较弱者（同上）

目标：作为突破口。

[image]

渗透者

告密者（线人）

[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image]针对反抗运动的政治渗透：政府线人如何操作

四、技术与策略维度

4.1 社交工程学的核心地位

报告强调：

本类攻击的核心不是技术漏洞，而是“人”的漏洞。

关键技术包括：

- 钓鱼攻击
- 虚假账号网络
- 内容操控
- 身份伪装

[image]

[image]移除你的绵羊墙：给普通人的5个防御课程

[image]什么是伪装，如何伪装，如何识破 — — 社交工程攻防基础

[image]袜子木偶 - 分身创建的小技巧

[image]宣传、审讯、渗透、操纵、诱导、伪装 ……关于欺骗和诡计您应该知道的一切

[image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”

4.2 与传统网络攻击的区别

报告认为此类攻击的未来趋势包括：

- 自动化生成内容
- 深度造假 https://iyouport.substack.com/p/079?utm_source=publication-search
- 大规模舆论操控 https://iyouport.substack.com/p/--c32?utm_source=publication-search

AI正在放大这些能力。

五、影响机制：心理、社会和政治层面

5.1 心理影响

受害者常出现：

- 不信任感
- 被监视焦虑
- 自我审查

这被称为寒蝉效应。

5.2 社群层面影响

攻击导致：

- 社群分裂
- 内讧冲突
- 组织瘫痪

这是叙事劫持的核心目标之一。

5.3 对家庭施压

一个关键机制是：

> 对境内的家属施压。这也是一贯做法。

例如：

- 威胁目标人的家人
- 经济处罚，等等

以迫使海外人士沉默。

5.4 政治影响

长期影响包括：

- 削弱跨国倡议能力
- 降低国际舆论影响
- 破坏人权网络

六、两大攻击行为体深度剖析

公民实验室通过长期的网络基础设施监测，识别出两个独立的攻击组织：**GLITTER CARP** 和 **SEQUIN CARP**。

6.1 GLITTER CARP：规模化的“初始准入者”

A. 行为特征与目标

GLITTER CARP 自2025年4月起活跃，其特点是“广撒网、重冒充”。

- 目标群体：涵盖几乎所有中国政府关注的敏感群体，包括维吾尔活动人士、西藏流亡组织、台湾媒体以及香港民运人士。
- 核心职能：公民实验室评估该组织在攻击链中扮演“初始准入者”（Initial Access Provider）的角色。他们的任务是窃取账号密码，随后将这些权限移交给其他负责深度监控或数据窃取的部门。

B. 攻击技术细节：身份伪装的艺术

1. 高可信度冒充：他们会冒充目标群体内部受尊敬的人物。例如，在针对维吾尔人的攻击中，攻击者冒充一名著名的维吾尔导演，通过社交媒体建立联系。

1. 钓鱼基础设施：该组织注册了上百个模仿合法机构（如独立电影发行商、科技媒体）的域名。

1. 虚假安全警报：如果初次钓鱼未成功，他们会立即发送伪造的“Google账号异常登录”提醒，诱导用户在惊慌中重置密码，从而进入虚假的登录页面。

1. 战术重复性：研究人员发现，尽管目标不同，但该组织频繁复用同一套服务器架构和钓鱼模板，这种“标准化作业”体现了其工业化生产的特点。

6.2 SEQUIN CARP：精准的“社交工程操盘手”

A. 行为特征和目标

SEQUIN CARP 的攻击更具针对性和耐心，主要针对报道中国跨境镇压议题的高级记者。

- 典型案例：对 ICIJ 记者 Scilla Alecci 的长期渗透。

B. 核心战术：叙事劫持和 OAuth 滥用

1. 劫持真实叙事：该组织最危险的地方在于，他们会窃取真实的、敏感的对话内容，并以此作为背景来构建虚假身份。例如，他们会冒充一个“持有政府内部绝密文件的举报人”，利用记者对独家新闻的渴求诱导其上钩。

1. **OAuth** 令牌攻击 ：

  - 原理 ：攻击者不直接索要密码，而是诱导记者点击一个链接，授权一个所谓的“第三方安全协作工具”。

  - 危害 ：这种授权一旦产生，攻击者就获得了该账号的 OAuth 令牌。这意味着即便记者开启了双因素身份验证（2FA），甚至修改了密码，攻击者依然可以长期、静默地访问记者的邮件、联系人和网盘文件。

1. 职业化沟通：SEQUIN CARP 的成员表现出极高的专业素质，能流利地使用行业术语与记者进行长达数周的“预热”沟通，降低其防备心理。

七、跨境镇压的“工业化”和私营承包商生态

报告深入探讨了中国网络攻击力量的结构性转变 —— 从“爱国黑客”到“商业黑客公司”。

7.1 军民融合战略下的激励机制

2017年后，中国正式确立“军民融合”为国家战略。这不仅涉及硬件制造，更包括网络空间能力。私营网络安全公司（如安洵 I-Soon、成都404等）通过竞争政府合同，获得了合法的攻击授权。

7.2 低成本和高效率的“黑客超市”

根据2024年泄露的安洵（I-Soon）内部文件，报告解析了这种生态的

恐怖之处：

- 按件计价：窃取特定东南亚国家部门的数据只需数万美元。对于中国政府而言，这种外包模式极其廉价且高效。
- 软件化和产品化：这些公司开发了成套的“钓鱼工具包”、“推特监控系统”和“地理位置追踪插件”，并像售卖商业软件一样卖给地方公安局和国安部门。
- 可否认性：使用私营公司作为代理人，使得中国政府在面对国际外交指控时，可以推诿为“民间行为”或“纯粹的商业犯罪”。

八、攻击行为对社会的毁灭性影响

报告不仅仅关注技术，更关注这些攻击对“人”的伤害。

8.1 破坏社区信任

攻击者冒充社区领袖（如著名的导演、活动家）的手段，在海外离散群体中播下了怀疑的种子。当成员们分不清谁是真正的同伴，谁是政府的代理人时，整个群体的凝聚力会迅速瓦解。

8.2 寒蝉效应和自我审查

长期的数字骚扰和潜在的家庭威胁，导致许多活动人士和学生选择噤声。这种“隐形监禁”成功地将一个国家的审查标准延伸到了全球。

8.3 对新闻自由的侵蚀

通过对 ICIJ 等机构的针对性打击，中国政府试图建立一种“恐惧威慑”：任何试图揭露政府内幕的记者，都将面临无孔不入的数字监控。这直接威胁到全球媒体对敏感议题的调查深度。

[image]

https://iyouport.substack.com/p/92d?utm_source=publication-searchhttps://iyouport.substack.com/p/as56-7?utm_source=publication-search

https://iyouport.substack.com/p/079?utm_source=publication-search

8.4 数字威权主义的新阶段

从“监控”到“操控”

传统数字威权：

- 监控

- 审查

新阶段：

操控认知与社会关系。

从“信息控制”到“叙事战争”

这标志着：

- 信息战 → 叙事战
- 宣传 → 渗透

从“国家行为”到“生态系统”

权力不再集中：

- 国家
- 企业
- 网络群体

形成了复合系统。

8.5 揭开跨国镇压体系

该报告是对中国跨国镇压模式的重要补充。

已有研究表明：

- 中国是跨国镇压最活跃的国家之一
- 手段包括监控、骚扰、信息操控等

本报告的贡献在于：

揭示其“信息与叙事层面的操作机制”

九、防御建议和政策应对

公民实验室在报告最后提出了针对性的防御策略。

9.1 针对高风险个人的建议

- 物理安全密钥（**Security Keys**）：如 YubiKey。它是目前抵御 GLITTER CARP 类凭据钓鱼最有效的工具，因为即便攻击者拿到了密码，也无法物理接触到密钥。

- 严格审查第三方授权：定期检查 Google 或 Outlook 账号中的“已授权应用”，撤销任何不熟悉的或长期未使用的 OAuth 权限。

- 带外验证（**Out-of-band Verification**）：收到来自“熟人”的敏感请求时，通过第二种通讯渠道（如见面、语音通话等）核实对方身份。

9.2 针对技术平台的建议

- 主动识别恶意基础设施：科技巨头应共享威胁情报，封禁那些跨平台复用的钓鱼域名。

- 增强 **OAuth** 透明度：当应用请求高级别权限（如读取邮件）时，系统应向用户发出更明确、更严厉的警告。

9.3 针对政府的政策建议

- 法律制裁：西方国家政府应对参与跨境镇压的私营公司及其高管实施定向制裁。

- 外交压力：将数字跨境镇压纳入双边外交议程，明确此类行为违反国际法和主权原则。

十：综合评估和局限性

10.1 报告的核心贡献

1. 提出“叙事劫持”这一关键概念。

1. 将跨国镇压从“技术问题”转为“社会问题”。

1. 揭示攻击的结构性与系统性。

10.2 方法论价值

- 结合技术分析与社会科学

- 强调受害者经验

- 构建攻击模型

10.3 局限性

（1）归因困难

难以明确：

- 国家行为体 还是 民间行为

（2）样本偏差

主要集中于：

- 特定群体（如维吾尔、藏人等）

（3）技术细节有限

更偏重社会机制，而非技术细节。

最后：一种“软性压制”的全球扩展

该报告揭示的不是单一攻击手段，而是一种新的权力模式：

> 通过身份伪装与叙事劫持，实现跨境社会控制。

其核心特征：

- 去中心化

- 低可见性
- 高心理影响
- 易于规模化

最终目标并非直接消灭反对者，而是：

> 让他们失去发声能力和组织能力。

这标志着数字威权主义进入了一个更隐蔽、更复杂、也更难以应对的阶段。

□

https://citizenlab.ca/research/how-chinese-actors-use-impersonation-and-stolen-narratives-to-perpetuate-digital-transnational-repression/

[image]

心理安全-PsychologicalSecurity

孤独可能是最大的风险因素。 “孤独”不完全指孤军奋战；更有，如果你随时需要拿出一部分精力来防备周围人（不论原因如何），你就很容易筋疲力尽，进而导致出错。 这种状况的可能性与您的工作的激进程度成正比。我们称之为“心理安全”。 心理安全是防御工事中的重要部分，毕竟“事在人为”，再精良的武器、再绝妙的战术设计，都不如一副理智机敏的头脑。

[image]
[image]

S04完美隐身-总章节：机智是重要实力

[image] 关键词	伪装 分身 社交工程攻击 袜子木偶 逃亡 隐姓埋名
[image] 关联	分身 [image]隐姓埋名 [image]假身份
[image] 创建时间	2025年2月1日
[image] **Description**	心理安全；行动安全性

我们的培训师将**S04**描述为“跑路者指南”，很幽默，一定程度上也的确如此。

不过**IYP**想说的是：如果您已经感受到跑路需求了，再开始**S04**那就来不及了。

S04就像防弹背心，您应该拥有，且能够熟练穿戴，它将大幅提升您的战术选择自由度。

S04 系列则是关于侦探/间谍和逃亡者的较量。

任何需要保护个人身份安全的人都应该了解这些知识。您将能从中发现，事实上在没有数字技术的情况下，也不难把一个试图隐藏的人“挖”出来。

心理学本身就是利器。

📌

本系列可直接服务于逃亡者（ [image]隐姓埋名 ）和反侦察前线（ 分身 ）。

鉴于安全措施最有效的基础在于操作的熟练程度，所以我们强烈建议您在“日常”压力最低的情况下执行整体安全最佳实践，这样您就可以逐渐熟悉安全习惯、并大幅减轻足迹积累。当危险真正来临时，您就可以轻松驾驭了。

[image]

您可能注意到了，与多数内容不同的是，S04系列同时存在于两个专题中：行动安全性和心理安全。因为它既是心理技巧也是行动战术。

本站“威胁知识库”专题的 “自卫措施”中包含3个策略与本系列相关：分身 、 [image]假身份 和 [image]隐姓埋名 。

对培训师说：建议将S04作为入门培训的一部分；即便您的团队没有任何直接行动的计划，了解一些心理对峙的技巧也非常有用。尤其是，防御既是一种智慧也是一种习惯，就像讲卫生的人不容易感染流行病那样，注重日常防御的人也不容易栽跟头。

在技术高端到不可思议的世界里，人力监视依旧有很多优势：它灵活、直接、易于调度、稳定、杂音少 …… 尤其是隐私保护措施已经越来越普及的情况下，人力监视尤其可以针对那些注意力被完全锁定在技术领域的人。

所以我们建议：各种☠镇压手段 您都应该了解。它们之间没有主次之分；最终您可能遇到什么，仅仅取决于您在对手眼中的“重要”程度和对手的资源能力。

在一些地方，私家侦探和赏金猎人的行业很火爆，甚至有些时候警方都会与这些行业内的高手合作，以挖出一个藏匿很深的目标人。

这些行业的人是拿钱办事的，所以您不用指望他们遵守什么道德。不论您所在的地方目前的状况如何，在个人隐私信息具有昂贵价值的时代里，这门生意火爆起来只是早晚的事。

私家侦探行业很疯狂，很多时候比警察更厉害；他们可能没有警察掌握的那些大型数据库，但他们具备高超的以骗制骗能力，有些时候比数据库都好用。社交工程师被称为人性骇客是有道理的。

🔑

对于激进派前线来说，最经常遇到的状况是：您的对手掌握所有大型数据库（👁🗨大规模数字监控 ）、还掌握着最先进的零日武器（□身份验证绕过 ）、而且还是心狠手辣的社交工程师。本站致力于帮您应付所有这些方面。

常言说得好，知己知彼百战不殆。如果您能知道对手最可能怎么做，您就可以做出最有效的防御。

列表

[image] 直面你的对手 - 6大原则：完美隐身S04E01

[image] 了解追踪者的手段和你的弱点：完美隐身 S04E02

[image] 思考方式是战略性的：完美隐身 S04E03

[image] 技术增值部分-最简单的分身方法：完美隐身S04E04

[image] 清扫和清点-信息篡改的重要步骤：完美隐身

S04E05

[image] 令人兴奋的心理过招：完美隐身 S04E06

[image] 大清洗 - 扫荡危险区域：完美隐身 S04E07

[image]
[image]

直面你的对手 - 6大原则：完美隐身S04E01

[image] 关键词	个人 伪装 免追踪 分身 社交工程攻击 袜子木偶 逃亡 防御 隐姓埋名 隐私
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月2日
[image] **Description**	心理安全；行动安全性

自由不只是有机会去做自己喜欢做的事；也不只是有机会在既定的方案中做出抉择。自由，最重要的是，有机会构建决策选项，争论其优劣 —— 以及，接下来的选择机会。

- Table of Contents

  1、您的个人信息是一种颇具价值的商品。不论您是谁，总有人对它感兴趣，总有人想要得到它。
  2、信息行业和其他行业一样。成功者懂得找到市场的空白点，而且懂得如何填补这些空白。追踪者之间的常态竞争能让强者更强。
  3、如果确实有关于您的任何精准信息，那么，只要他们有足够的时间和精力，追踪者肯定会能把您挖出来。
  4、任何公司只要有客户代表的人工服务，那么一个好的追踪者需要的就只有两种东西：一部预付费电话，和魅力。
  5、一名优秀的追踪者可以从任何一个持有信息的人那里获取信息。他能轻松地做到让您将价值连城的信息视为粪土。
  6、也是最后一个原则：追踪者在操作中可以犯几十个错误；但您只要犯一个错误，您就over了。

[image]

欢迎来到猫鼠游戏。

第一条规则是：

如果你很容易被抓到，说明你还不够聪明。

希望S04系列能帮您变得更聪明。因为本系列将从赏金猎人的视角出发 —— 让您看到一个专业的追踪者都会干些什么、如何思考，以便能作出最有效的防御。

对于任何一种斗争来说都是如此：你能做到的避免被对手了解的程度越高，你就会越安全。

[image]

现在进入正题：关于追踪的几个原则 —— 即 追踪者熟知并秉持的东西，反追踪需要了解的基础。

1、您的个人信息是一种颇具价值的商品。不论您是谁，总有人对它感兴趣，总有人想要得到它。

很多对个人权利表示“无所谓”的人，基本都是因为觉得自己“没有权利”。这不是事实。这只是想要控制您的人灌输给您的概念。

因为只有您放弃了个人权利，那些想要控制您的人才能成功。

延伸：https://iyouport.substack.com/p/--dd7?utm_source=publication-search

个人信息是一种至高无上的权利。也许您自己对自己的个人信息太熟

悉不过了，于是觉得“它没什么稀奇的”；但是，对任何其他人来说都完全不同。这也许是很多人误解个人信息之价值的原因。

不论是罪犯还是守法公民，在此都一样。您肯定还不知道自己在追踪者眼中有多么的价值连城。

不论是想要找到您的真身、还是想要盗用您的身份，那个人绝对会不惜一切代价做到这点。

□

延伸：https://iyouport.substack.com/p/-7?utm_source=publication-search

如何才能让一个人感知到个人信息有多值钱？

方法很简单，那就是，让TA 尝试一下私人侦探的业务 。

还记得我们在开源情报中多次强调过的吗：它既可以进攻，也可以防守。同样道理。

开源情报市场已经高达数十亿美元，这可是仅仅基于开源的情报市场；私人侦探就更不用说了，他们游走在黑白之间，他们可以采取任何可用的手段，只要没被抓到，钱到手就是合法的。

这一行业内的成功者都是不会按理出牌的人；他们经常可以自如地跳出常人的思考框架做出那种能让您意想不到的事。

□

延伸：https://iyouport.substack.com/p/lr-iyp?utm_source=publication-search

于是这就引出第二条原则：

2、信息行业和其他行业一样。成功者懂得找到市场的空白点，而且懂得如何填补这些空白。追踪者之间的常态竞争能让强者更强。

就如上面所说到的，这一行业拿钱办事，谁出的价码高，就接下谁的活。（这很容易理解，混过 Hack Forums 或逛过零日市场的人都知道）

如果被追踪的人是您，对手出价越高，您就离死神越近。

永远不要停止惊讶于社交工程师的创造力，他们就是靠创造力吃饭的。

延伸：https://medium.com/@iyouport/%E5%8F%AF%E6%80%9C%E6%AD%A3%E4%B9%89%E6%B2%A1%E6%9C%89%E9%92%B1-d3bec8596c6c

3、如果确实有关于您的任何精准信息，那么，只要他们有足够的时间和精力，追踪者肯定会能把您挖出来。

随着技术的进步，追踪行业的钱只会越来越好赚，越来越简单和高效。

他们不需要具备骇客能力，甚至不需要懂编程，因为最大的漏洞永远是人；社交工程之所以被成为人性骇客，就是这个道理。

只要有足够的胆量和创造力，您就能拿到您想要的东西。

这说明了第4个原则。

[image]

4、任何公司只要有客户代表的人工服务，那么一个好的追踪者需要的就只有两种东西：一部预付费电话，和魅力。

很简单：正因为人是最大的弱点。

与其钻研复杂的数学、购买昂贵的0-day，以寻求技术层面的漏洞，不如直接针对最明显的漏洞，即 人性。

这就是私人侦探一直在做的事 —— 漫天的借口和谎言、加上真诚可亲的个人魅力，以及严谨的逻辑和专业知识，这些是最强大的武器。

尤其是我们曾经在“伪装术”中介绍过的要点：您可以伪装成任何人，从流浪汉到苏格兰场高级探员，从家庭主妇到白宫秘书，但您必须能做到“变成”那个人，而不仅仅是“伪装”。

[image]

返回：[image]什么是伪装，如何伪装，如何识破 — — 社交工程攻防基础

我们在这里说的事听起来很简单，但现实生活中极少会有人真正能做到“冒充”他人，尤其是冒充拥有强大权力的人，然后随便给各种公司和政府部门打电话，支配对方做任何奇怪的事情，现实中这非常罕见；但真正的社交工程就是这样做的。

也正因此，电话那一端的人很少会产生怀疑。尤其是，您自报的头衔越高，对方信任您的可能性就越大。

要知道接线员都是些资历很浅的员工，虽然如今很多部门会对所有员工进行反社交工程攻击的培训，但培训毕竟不是实战，修补人性漏洞的效果并不高。

这也是最可怕的部分：如此简单的行骗伎俩如今依然屡试不爽（如果您接触过专业的渗透测试公司/团队，可以问问他们，真的是这样）。

也就是第5条原则：

5、一名优秀的追踪者可以从任何一个持有信息的人那里获取信息。他能轻松地做到让您将价值连城的信息视为粪土。

这里所说的“任何一个人”包括您的邻居、保姆、您父亲母亲、您居住的小区物业的清洁工 …… 您最常去的杂货铺的小老板，等等一切。

在中国，任何一位与国安部门（情报部门）或高级警探打过交道的人都能了解这点，无需过多解释。

还是那句话，人们经常不会觉得自己的特征有多值钱，或者说基本想不到也不会去想自己在他人的印象中是什么样 —— 但这正是最大的弱点，是社交工程师最容易的切入点。

[image]

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

举个简单的例子。我的一位朋友是土生土长的英国人，他在冰岛工作了3年之后再回到英国。他曾经满脸惊讶地告诉我，他以前居住的地区的杂货铺老板看到他时说：“好久不见，你黑了，头发也长了”……

因为他住在英国的时候从未与那间杂货铺的老板交流过，他就如我们所有人一样，只是买东西、付款走人。他很难想象一个“陌生人”会在3年后还记得自己曾经的样子。

然而这就是事实。

想象一下，如果我的那位朋友是被情报官员、私人侦探和赏金猎人关注的目标，结果会怎么样？……

别急，我们将在本系列中介绍几乎所有防御办法。

[image]

再说另一个真实的故事。

一位多金的大客户打了一个电话给私人侦探公司的社交工程师，给了后者一个女人的名字，他们想要知道这个女人在哪。

只有一个名字。

这些社交工程师就开始使用常规钓鱼方法打电话给各种公司，一概声称自己是那位女士，询问对方的服务并声称自己搬家了、注册地址已变 …… 不久之后就找到了那个女人可能的藏身地点。

接下来就是给这个可能藏身的地方打电话。接线的人是她家保姆。以下是对话：

社交工程师：您好，我是 UPS 快递公司的***，我们有她（那个女人的名字，故意读错她的名字）的包裹，但是包裹进水了。我们非常抱歉！

保姆：哦，那么…

社交工程师：我们需要她签名才能处理，不知道她什么时候会回来？

保姆：啊……

社交工程师：那好吧，我们把包裹退回去就行了。

保姆沉默了一会。

社交工程师：我们可以把包裹退回去吗？

保姆：不……不要，你直接送过来吧。

社交工程师：好的，那么我们什么时间可以找到她签名？

保姆：她六点左右会回来。

搞定。

以上对话部分中深颜色的字意味着需要重音读出 —— 这是心理操纵的逻辑。

目标人将于某某时间到达某某地点 —— 这条信息交给那个多金的大客户，钱就到手了。

那么，那个女人究竟是谁呢？

如今几乎所有人都知道她，她就是莫妮卡莱温斯基（Monica Lewinsky）。

您一定还记得我们正"战略性欺骗"中指出的：只要进行了欺骗，就存在被发现的可能。区别只是在于，发现的时间，是及时、还是为时已晚。

社交工程欺骗也一样，它很容易被揭穿，而且很容易漏出马脚 —— 不同的只有，是及时、还是为时已晚。 只要您能争取到时间，就是绝对的胜利 。

[image] 西班牙剧集"La Casa de Papel"的剧照。该剧值得推荐，其中展示的社交工程和心理战策略非常标准，简单易懂。

时间和时机是在社交工程战术中价值连城的东西。

6、也是最后一个原则：追踪者在操作中可以犯几十个错误；但您只要犯一个错误，您就over了。

职业社交工程可以充满娱乐性，我们绝对不是鼓励您加入这一职业；而是，想要通过对这一职业的解剖，帮助您避免被追踪。

请务必牢记上述6个原则。

这里是开篇。

也就是说，如果您正在着手准备一套“退出”策略 —— 保护性策略，那么必须以这**6**大原则为前提。

[image]

返回：[image]隐姓埋名 —— 当您准备采取该主题策略时，S04系列就是您的护身符。

本系列内容就是希望帮助您制定这样的策略，您可以在任何必要的时候“重返”现实；在不必要的时候销声匿迹。

[image]
[image]

了解追踪者的手段和你的弱点：完美隐身 S04E02

[image] 关键词	免追踪 数字卫生 数字足迹 社交媒体 社交工程攻击 自检
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月3日
[image] **Description**	心理安全；行动安全性

小心驶得万年船。

- Table of Contents

  1、对于任何一家想让您的生活变得更加便利的公司，都应该敬而远之。
  2、社交网络、搜索引擎、病毒式媒体，都是个人隐私的最大敌人。
  3、您永远不会知道互联网上的所谓“好友”都是些什么东西。
  3、与其在网上，不如在现实生活中实行个人兴趣爱好。
  4、点击“发布”之前请三思。哪怕日后您删除了账户，凡事只要上了互联网，就基本很难撤销了。您需要从一开始就特别谨慎。
  5、公司客服越善良、越容易交流，就越容易上当受骗。

[image]

也许您很幸运，可以负担得起水电以及生活中的一切便利；还可能更幸运，买得起电脑，可以上网，在 Facebook 和 Twitter 跟一群人扯蛋；还有便捷的在线金融服务、电话公司、电力公司、宽带公司、以及各大公司提供的优越在线客户服务……

各家公司争先恐后地想要标榜自己有多么地“用户友好”。全天候的热线电话、无微不至的关怀。您会感叹：世界真美好啊。

抱歉，忘了说了：以上是追踪者的感叹。

欢迎来到E02。本集的主题就是：客户友好型公司不是您的好友，而是追踪者的好友。

联邦调查局第一任局长约翰·埃德加·胡佛在历史上已经树立了一个坚固的反乌托邦标志 —— 胡佛先生因骚扰侵犯政治异议人士和活动家、搜集政治领袖的秘密档案、以及采取各种非法手段收集证据，而闻名于世界。

自从那个年代开始，侵犯个人隐私的罪魁祸首就是群众斗群众 —— 互联网时代将群众斗群众自动化了，并且笼络了跨地区、甚至跨国的群众，任何人都能卖了您。

所以，如果您想要隐身，首先要做到的就是：

1、对于任何一家想让您的生活变得更加便利的公司，都应该敬而远之。

现如今每一家大公司基本都是如此，网站则更甚。

当一个中年人想要找到几十年没联系过的小学同学可以易如反掌的时候，想要隐身就不那么简单了。

当然，前提是您要把电子邮件、地址、电话号码、个人照片、家庭照片 …… 统统上传到网站，供全世界的人观看。对这些东西感兴趣的人中**99%**都是社交工程师，如果足够幸运，剩下的1%是您希望联系的人。

在线电话薄、博客、互动式网站、病毒式营销广告…… 也都是如此。

尤其应该关注的还包括：大型国有水电企业、电话公司、互联网公司，等等，专业的追踪者经常通过这些地方获取重要信息：随便找个借口就可以撬开那些接线员的嘴。

延伸：https://iyouport.substack.com/p/a20?utm_source=publication-search

延伸：https://iyouport.substack.com/p/cb1?utm_source=publication-search

客户越是容易接入在线人工服务，追踪者就越容易对其造成真正的伤害。

如果任何一家公司了解您的真身，您都应该非常小心。

[image]

返回 - 自卫措施：分身

如果您觉得分身法不适合您，同时您还希望隐身，那么就要避免使用任何上述这些服务，彻底远离互联网。您觉得哪个更方便呢？

2、社交网络、搜索引擎、病毒式媒体，都是个人隐私的最大敌人。

追踪是一种非常古老的行当。而如今想要在互联网上找到一个人的信息，您完全不必成为一个黑客（您甚至可以一点技术都不懂），照样能搞定。我们的开源情报栏目中很多实现靠的都是思考方式，而不是技术。当然，有技术会更好，至少您会使用其他人开发的技术，可帮助追踪工作提速。自动化是个好东西。

一旦嗅到您的气息，追踪者要做的第一件事就是想方设法打入您的社

交关系网。

您经常去的公司是哪里、经常出入的场所都包括什么、经常和谁混在一起 …… 对追逐者来说这些都是非常重要的目标。

接下来社交工程师就会开始行动了，打电话、发邮件、搭讪，直到有人上当，吐露了最重要的信息 —— 而社交媒体网站将所有这一切都变成了一站式服务。

[image]

返回：[image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”

只要您有 Facebook（包括所有类似的社交媒体），即便您进行了高度严格的隐私设置，您的个人主页依旧是一座金矿。

除非您的隐私设置为最高级别，否则任何陌生人都会能看到您的好友清单，哪怕他们还没有添加您“好友”。

一旦添加成功就更厉害了。社交工程师的袜子木偶经常这样做。

您可能会说，“陌生人只会看到部分好友啊”，没错，但是，只需要点击刷新，就可以积少成多。因为每次刷新后好友信息都会有所不同。这是最傻瓜的做法，但很有效。

Facebook 是间谍的金矿，但绝对不是唯一一个金矿；所有社交网络、媒体、博客、购物网站、支付平台**……** 都是。

社交网站都喜欢爆料，不论您选择了什么样的东西挂在网上。优秀的追踪者都可以用来对付您。

他可以冒充一个想和您取得联系的“老熟人”，添加您的朋友和家人为“好友”。

任何遭遇过国家情报部门间谍活动的人（不论是在中国还是美国还是欧洲）都应该很熟悉这种手段，这是间谍们的套路之一。

[image]

返回：扮演追逐者，抢先检查一下自己在网上泄露了些什么东西
[image]自我人肉

[image]

3、您永远不会知道互联网上的所谓“好友”都是些什么东西。

避免的方法很简单：如果您打算同意添加某人为好友，哪怕这个人是您非常熟悉的老朋友，也要记得，给对方打个电话对他们表示感谢 —— 目的是借此确认对方是不是真的。

一个人多年杳无音信，忽然之间跑到网上要加您“好友”？这种需要格外小心。

一位社交工程师讲过一个故事。那还是社交媒体火爆之前的事。

某次社交工程师接到一个生意，需要寻找一个人A，A是一名卡车司机，据称其谎报受伤，申请残疾保险。

社交工程师对A进行了广泛的监控，但是一无所获，没有发现关于他的任何欺诈行为。

A看起来是个失业人士，而且非常隐蔽，住在一个破烂不堪的拖车公园里。谷歌搜索他的名字以及多个变体，还加上出生年月，最终才在一个校友网上看到了一则寻人启事，其中A说要想要寻找失散多年的中学女友。

然后社交工程师的机会就来了。

他们使用寻人启事的联系方式与A取得了联系，声称自己就是那位失散的女友，还诉说自己婚姻的不幸，很高兴A还记得她……等等。

很快就收到了回信。A写了好几页，满满都是爱意。

一系列邮件往来后，A产生了一些怀疑，他要求打电话聊一下。社交工程师婉拒了，称“她”丈夫有家暴倾向。A做出了让步。

A穷困潦倒，住的地方连电脑都没有，每一次接收假的“她”发来的邮件，还需要跑到图书馆去借用电脑。有一次A在回复邮件时提到，为了等待“她”的邮件，他在图书馆里整整坐了4个小时。

在邮件中，A对自己的生活不太隐瞒，但是只字不提在哪里工作，并且他一直坚称自己身患残疾。

欺骗总会被发现的，A的怀疑似乎加深了，他要求见面聊。社交工程师顺便问：“哪里见面”，A便给出了路线和日程安排。

这就是社交工程师用来换钱的东西了 —— 那位寻人的客户在该日期到来时，题着一部相机坐上了A指出的那辆巴士。

最终，A因谎称残疾骗保，犯有欺诈罪，要在监狱里待一段时间了。

很多人都和A一样，使用社交网络只是出于某种兴趣爱好，不论是公仔、猫咪、国标、汽车、名酒、还是任何话题；如果您也有某种兴趣爱好，那么您应该进入真实的世界，在社区俱乐部里或旅行中满足自己，而不是跑到社交网络上。

否则，您的任何爱好都会最终成为您的枷锁。

3、与其在网上，不如在现实生活中实行个人兴趣爱好。

这条原理很奇怪吗？一点也不。有人曾经就因为追星，而被社交工程师擒获。

那位中招的女士迷麦当娜。

她是一家公司的雇员；摔了一脚，于是提出残疾保险申请，并且起诉其雇主玩忽职守。其雇主认为此人并非摔伤，于是聘请了私人侦探对其实施监控。

她非常谨慎，从来没有在院子里活动过，也没有找新工作，可以说没有做任何一种能让她暴露其现状的事。普通监视方法失败。

没关系，社交工程师开始在网上挖掘关于她的东西。很快就在一个麦当娜粉丝签名簿里找到了她的名字。由此还找到了“我的空间”网中她的网页。

于是社交工程师给她写了一封信，说她赢得了一项大奖，有机会让她和其他获奖者一起竞争参与麦当娜录像的机会。

社交工程师给她发了一个网址还有一个电话号码；两者都含有比赛信息。网站是在一家海外私人企业注册的，通过预付费卡支付的费用，电话号码则是一个预付手机号。于是她无法追溯到来源（哪怕她知道该怎么做）。

[image]

返回：当您需要购买敏感服务时也应如此，严格遵循 [image]数字技术限制和最佳实践

这位目标人很快就中计了。社交工程师告诉她比赛规则，包括试镜。

在试镜的那天她果然来了，填写了一张表格；社交工程师要求她提重物、做了几次开合跳、仰卧起坐，还有一些舞蹈动作 —— 所有这一切都被录像了。

她的工伤赔偿金彻底吹了。

兴趣爱好是定位目标人的最可靠途径。一旦您的小爱好被社交工程师了解到，他们就会想方设法寻找那些能帮您维系这些兴趣爱好的地方和人。

如果您不想中这种伎俩，那就要注意：千万不要把真实的自己都放在网上。互联网的可怕肯定比您想象中更大。

[image]

4、点击“发布”之前请三思。哪怕日后您删除了账户，凡事只要上了互联网，就基本很难撤销了。您需要从一开始就特别谨慎。

一个网页就可能带来极其严重的危险，并且没有人知道网页究竟会存在多长时间。

延伸：比如，通过这里提供的工具做个初步体验 https://iyouport.substack.com/p/15f?utm_source=publication-search

但更可怕的是，在社交网络上，个人对自己的页面几乎处于完全失控的状态。即使您注销了账户，只要任何认识您的人依旧在网络中，他们中任何一个人都会在无意中出卖你。

别埋怨他们，他们很可能并没有意识到自己这样做是有害的；您自己也很可能尚未意识到互联网上还存在关于您的真实信息 —— 那些给社交工程师的攻击行动提供的弹药。

这就是为什么我们要强调，在准备做一切“大事”之前（包括并不限于隐身），您应该至少执行以下：

[image]

返回：[image]自我人肉

返回：[image]少即是多：变得难以被追踪的简单方法 S03E05

返回：[image]在雷达下低飞：变得难以被追踪的简单方法 S03E07

请记住：追踪者都是专家级的社交工程师，他们只需要使用传统的方法（非高端技术）即可做到掌握您的致命信息。

于是您要记得……

5、公司客服越善良、越容易交流，就越容易上当受骗。

一个人越是健谈、容易和陌生人闲扯，就越容易被糊弄。关键在于如何拉近与人之间的关系 —— 这就是社交工程的重点能力。

您可以参考以下内容：

[image]

返回：👄语言是强大的武器 - 如何使用它？人性黑客：致命的诱导

当然这不是全部，“全部”非常复杂，尤其包括很多随机应变的灵活性，这需要来自于经验。

[image]

以上这些是最基本的部分，但如果您能全部搞定，就可以绕避大多数追踪者。

开源情报是社交工程师的生命线，使用开源情报的熟练程度是成功的关键；反过来，如果您不想遭遇社交工程攻击，就非常有必要熟悉开源情报的操作方法，这样您才有可能从根本层面上做到抵御。

社交工程训练很复杂，也可能很有趣；其中包括对战测谎仪。

[image]

返回：[image]如何欺骗，和如何防骗：反侦基础课 S06E07

您能欺骗测谎仪吗？如果能做到，将可以成为一位令人敬畏的社交工程老贼。

反过来，如果您是防御者，不要期待通过教科书上告诉您的识别谎言方法去揭穿社交工程师，因为那些方法距离测谎仪的水平还差十万八千里呢；您需要做的是以牙还牙、以骗制骗，以同样的方法反击回去。

斗智是令人愉快的。尤其是当您赢了的时候。

[image]
[image]

思考方式是战略性的：完美隐身 S04E03

[image] 关键词	分身 反侦察 反追踪 社交工程攻击 自卫 逃亡 隐姓埋名
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月4日
[image] **Description**	心理安全；行动安全性

现在，开始消失吧……

- Table of Contents
说在前面
时间节点
原理
信息篡改
信息杜撰
信息重组
第一步：信息篡改
下一步

[image]

本集的内容是，开始行动。

说在前面

不论如何，如果您是一个极为重要的人，您的对手会不惜余力地找到

您；并且如果您的对手非常有钱且有大把时间，那么他们绝对会用尽一切办法。

但阅读本文的绝大部分读者都不会是那种极为重要的人 —— 于是，多数情况下，只要您能在追逐和反追逐中抢到足够的时间，您的对手就有可能耗尽耐心和钱财，从而结束战斗。

时间 —— 就是这场斗争中最值钱的东西之一。

如何赢得时间？

其实很简单，使用的就是我们在“战略性欺骗”系列中强调的攻心策略。您可以在下面回顾：

延伸：https://start.me/w/1w7j8l

战略性欺骗系列内容的使用范围非常广，关于欺诈、虚假消息、恶意诱导、洗脑、操纵、心理战对战策略 ……以及追击和反追击技巧等相关问题，都在里面。只是不会纳入本站。

每一种对峙都是心理战：因为，只要您能让对手失去反击的能力和信心，您就赢了。反之亦然。

在追击和反追击中可以有无数个拐点 —— 自然产生的以及人为促成的 —— 在每一个拐点上您都可以运用“战略性欺骗”技巧，将对手引入错误的方向。

时间节点

如果事出很急，您想要立刻逃离，那么您最想知道的也许是：需要多

久的准备工作？

事实上这取决于您愿意舍弃多少。

如果您有很多钱，而且全部想要带走，那么时间就会相对较长 —— 您想带走的东西越多时间就会越长；如果您孑然一身，并且熟练操作，两周甚至一周内就可以消失了。

[image]

原理

先讲一个故事，是一个经典小说，小理查德·康奈尔的《最危险的猎物》。

故事的主人公是一个叫雷斯福德的家伙。他被困在了一个小岛上；和他一起被困在这里的还有一个非常绅士但又非常疯狂的老者 —— 扎洛夫将军。

将军的爱好是：狩猎活人。

不久之后雷斯福德就在森林里一路狂奔 —— 他成为了全世界最狗屎的野生动物园里的最新战利品。

一开始他脑子里只有一个想法，那就是：和扎洛夫将军保持距离。为了实现这个目标，他一路狂奔，激励着他的是一种近似恐惧的东西。

但是现在，他终于能冷静下来了。他停下了脚步，开始思考自己，思考自己的处境。

他明白了，毫无目的地飞奔是完全徒劳的；最终他将不可避免地和大海面对面。四面环海的岛屿是个天牢。

他想明白了，他需要做的是给追击者留下一些可以寻觅的踪迹 —— 以将其引向错误的方向。

雷斯福德偏离了崎岖的小径，投身于毫无路径可言的荒蛮之中。

他精心设计了一系列圈套；他一再重复着自己的足迹。就像民间故事里总是能最终逃脱的狐狸……

故事结尾不重要，重要的是：雷斯福德处心积虑的谋划最终取得了成效。他知道，要做到成功的销声匿迹，就必须：有一点狡猾、有一点欺骗，要尽你所能去除一切真实的痕迹，并同时，设置虚假的误导性痕迹，让你的追逐者偏离方向。

[image]

返回 - 在“自卫措施”中，这一技巧被称为 [image]反监视 ，也就是甩掉跟踪的尾巴

这就是完美隐身的关键思考方式。

这是一个三步策略：信息篡改、信息杜撰、信息重组 。

信息篡改

首先就是[image]自我人肉 。尽可能找到所有与您自己有关的信息线索，

然后运用各种删除方法尽可能清除掉这些信息；如果无法清除，那么就想办法给它们改头换面，目标是追踪者无法据此对你定位。

信息杜撰

也就是战略性欺骗部分了。给追踪者设置虚假的线索路径，尽可能地为自己争取时间，并同时无限地消耗追踪者的财力和精力。

必须要巧妙。

要知道大部分追踪者会花钱聘请专业侦查团队，或者他们本身就是政府当局，拥有强大的情报能力。

但不要被专业头衔吓住，因为他们和您一样都是人，人类天然具备的思维弱点他们身上都有。

心理战术的关键就在于：谁先拿下对手的弱点。

有多少种追踪方式就有多少种反追踪方式；您要做的就是无限地消耗对手，直到对方因枯竭而放弃。

信息重组

开创新的生活，享受私密的生活，隐秘的住所，不留下一丝线索。

[image]

返回 - 在“自卫措施”中，这一阶段被称为[image]隐姓埋名

采取 分身 策略可以在数字世界帮您找到安全之地。而在现实中，您还需要一些其他东西。

三步完成就是自由的世界。

由于篇幅原因，本文只介绍第一步；后面的部分将另开新篇。

[image]

第一步：信息篡改

任何一位不想要生活在1984里的人都应该学会信息篡改。

“知己知彼，百战不殆”。信息篡改背后的原理就在这句话中：抢在对手的前面了解自己的弱点，以及对手的意图，才能抢得先机，防患于未然。

辨别并销毁一切外在的、与你有关的信息

如果不能销毁，可以与信息提供者取得联系，随便撒个谎，告诉他们档案中的信息错了，您想“更正”信息。由于肯定不会有很多人去把关于自己的真相改为假象，于是理论上很多公司部门不会怀疑您的说法。

其目的在于混淆视线、误导、将任何一个试图监视你的人都引向其他方向。

效果最好的时候，这种做法可以让追踪者裹步难行；效果最差的时候，追踪者也需要反复找借口、用尽一切搜索手段，才能找到您真正的位置。这种搜索方法既耗时又费钱。如果您幸运，对手会因此被掏空，耐心耗尽。

一个细节就是：别在法律的框架内思考问题。这是维权人士经常出现的错误。他们认为“这是非法的”，于是对手“做不到”。但对于反追踪来说，绝对不是如此。

不论您的对手是政府当局、情报部门、还是私人侦探，在此都一样，在追踪的操作中违法的可能性非常高，因为违法是他们的优势。

而作为反追踪者，您的工作就是尽可能发挥想象力去预测对手下一步会做什么，然后提前下手，给对方挖坑。

比如美国的 Zabasearch 或者中国的“找人网”，这些对方都是很高风险的 —— 使用独立的设备 + VPN/Tor + 虚拟机，去那里搜索自己，记录下找到能找到的任何东西，写在纸上而不是在线保存，然后逐一破解或混淆它们。

[image]

返回 - 特别强调在做这件事的时候请遵循数字最佳实践

完成后别忘了把那张纸烧掉。

[image]

在美国您无法完全屏蔽个人公开信息，除非您有切实的证据受到了人身威胁并据此去申请法庭指令。想必在中国也差不多。但至少您能做到为对手增加侦查的难度。

去每一个您能找到的在线数据库和电话簿看一眼，找找看上面多少关于您的信息。这就是最基本的自我人肉。

如果您不熟悉加密技术、虚拟机、彻底清除指纹的诸多操作，那么建议您在整个过程中使用纸和笔记录信息和进行思考，而不是使用在线工具。用完后将所有纸烧掉。

搜索自己的名字，以及名字的各种变体，名字加地址，名字加公司，等等；这就是追踪者一开始投入时会使用的方法。尽可能删除您能找到的任何东西。

然后，为上述每一个搜索条件都创建一个谷歌提醒，一旦有人在互联网上输入了某个具体的搜索条件相关信息，谷歌就会提醒你。你也可以使用这个方法确保在信息篡改后没有人再重新添加关于你的信息。

[image]

返回：[image]如何知道有人正在线人肉你？6个简单的方法

搜索条件就是姓名、位置、工作单位以及不同的组合，比如这样：

- 张三疯
- 张三·疯/峰/丰/风…
- “张三疯”
- 张三疯 ＋ 北京
- 张三疯 ＋ ABC有限公司
- 等等

如果电子邮箱是“zhangsanfeng@fakeaddress.com”，你可以这样：

- 张三疯 AT fakeaddress
- （张三疯）（fakeaddress）
- zhang (DOT) sanfeng (AT) fakeaddress (DOT) com
- 等等

确保删除所有照片，卸载社交媒体；在卸载之前取消掉对所有与你真实相关的人的关注；清除掉所有与你主页相关的链接。

如果您的朋友很多，慌乱之中有可能遗漏，没关系，可使用下面工具查找自己可被搜索到的社交关系网。然后清除它们。

延伸：https://t.co/SGQmIkjHtH

就算您逃出本国，找到您也不是那么难；因为这是社交网络时代，人们的亲朋好友同事熟人都在迫不及待地在互联网上公布含有您的照片；这绝对是您的灾难。

请务必告诫自己周边的人要多一个心眼。最好的是您自己不要亲自公开任何真实的东西。

想想看，任何地点还有哪些关于您的个人信息？一般来说社交工程师会最先从以下这些地方找线索：

- 电话公司
- 移动公司
- 家居商城
- 电力公司
- 健身房
- 有线电视服务商
- 卫星服务商
- 互联网服务商
- 租赁店和租赁服务
- 杂货铺和超市（会员部）

- 旅游公司
- 沙龙和校友会
- 银行
- 信用卡公司

您在上述这些地方是否有账户？给他们打电话，删除自己的账户，最好是能篡改部分信息。

下一步

进行到这里很多人也许会觉得非常凌乱，因为人们对谎言的记忆需要很大的努力。不过没关系，您完全可以提升记忆力；那就是下一部分的主题：关于如何将所有漏洞都堵上。

[image]
[image]

技术增值部分-最简单的分身方法：完美隐身 S04E04

[image] 关键词	IMs 分身 匿名购买 反追踪 手机号 数字足迹 电邮
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月5日
[image] **Description**	心理安全；行动安全性

重生自己。

- Table of Contents

  掌握本指南，您需要的东西：
  难度
  第**1**步：获取与您的个人信息完全无关的电话号码
  有关您设备的重要说明
  缓解措施
  第**2**步：获取与您的真实身份分离的电子邮件地址
  重要准备：使用安全的 **VPN**
  第**3**步：设置 **Twilio** 号码以创建无法追踪的在线帐户
  在 **twilio.com** 上创建一个帐户
  登录 **Twilio.com**
  在 **Twilio.com** 上创建您的试用版号码
  开始创建应用程序账户
  将试用版号码升级为付费帐户
  使用 **Twilio** 号码启动 **Telegram** 帐户

匿迹并非彻底销声。

很多情况下您必须“活着”。不仅为了避免陷入严重的心理障碍危机 —— 离群索居的压力会非常大，有可能是一种残害；并且，您的确需要一个新身份开启新的生活。

[image]

S04 系列以现实中的反追踪技巧为主，但必然会包括在线追踪的抵制方案。因为在线追踪是现代追踪者最常用的手段之一。

总之，对于您来说，不论是现实中还是数字世界，都应该做好充分的防御。

特别强调：相关方法和工具的更新换代可能很快，但思路不会变。您只要掌握思路，随时都能找到新的工具作为替换。

[image]

返回 - 从威胁矩阵索引进入该主题 分身

开始模拟操作。

掌握本指南，您需要的东西：

- 找到1张visa/万事达卡礼品卡，或与您完全无关的信用卡。
- 1个与您没有任何关系的新的/未使用过的智能手机（可选，但如果能有会更方便）。
- 1个连接互联网的设备，笔记本电脑或台式机。这台机器不是您的，也不会追溯到您。
- 0基础知识。

- 2小时的时间。

难度

低到中等。

[image]

不论任何理由，如果您打算创建一个或多个新的身份，以隐藏真实的身份（例如，如果您是政府网络间谍的目标，为了防止被他们跟踪或欺诈），您都需要一个他们无法追踪到的帐户，以便您可以保持安全，不论是在线还是离线。

当互联网允许您成为您想要的任何人时，曾经做到这点并不难。但是，现在不行了，因为监视资本主义正蓬勃发展。

这意味着所有在线服务都在试图使用各种方式来收集您的个人信息，描述您，跟踪您的工作，并从您的所有数据中赚钱。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

对于应用程序来说尤其如此。多数聊天应用或社交媒体都会要求您提供手机号码来创建或验证帐户。

电话号码是个非常危险的东西，能够让任何目的的追踪者顺利找到您，尤其是政府间谍。即便不是政府间谍也不难通过电话号码挖掘关于您的身份信息。

[image]

返回：[image]如何不暴露手机号、不花钱，实现双因素身份验证？

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

在本指南中，您将了解到如何创建无法被追踪的在线帐户，保护您的真实身份。通过三个简单的步骤即可实现：

- 获取与您的个人信息完全切断的电话号码；
- 创建一个与您的真实身份完全分离的安全电子邮件地址；
- 使用它们为您想要的任何新帐户获取Twilio号码。

第1步：获取与您的个人信息完全无关的电话号码

在创建新的在线帐户时，您通常需要一个号码来接收验证短信或电话，然后才能使用该帐户。

由于您会持续需要此号码来控制帐户，因此您无法使用公用电话或朋友的手机号码。

您需要一个专用号码，只有您可以拨打电话或接收短信。

这个号码必须很难被追踪，即便在当下追踪方法如此高明的情况下。

要生成这样的号码建议您使用名为 Twilio 的工具。与其他服务相比，Twilio 的维护成本更低。

要设置 Twilio，您需要一个电话号码和一个电子邮件地址。下面将引导您完成注册。

先从电话号码开始。

有两种获取电话号码的方法：购买SIM卡（如果可以的话）、或获取虚拟号码。

一定要使用现金购买无需身份验证的**SIM**卡。因为正常的电话号码可能与您的大量私密信息相关联，甚至包括您的实际位置。

[image]

返回-工具：[image]私密电话号码

返回-工具：[image]虚拟手机号和马甲邮箱隐藏真实信息

使用此SIM卡的号码和未连接到您的真实身份的新/旧手机，您已经可以制作与您的个人身份信息完全无关的帐户，如 telegram、Signal、Whatsapp、等等。

但是，维护此SIM卡可能会很贵。最好只将它用于创建一个 Twilio 帐户。

在以下步骤中，您可以找到如何设置、使用和维护 Twilio 号码，而无需依赖此SIM卡。

有关您设备的重要说明

在手机上使用此SIM卡或使用手机进行在线活动之前，需要了解一些重要事项。

首先，您要避免将日常使用的 SIM 卡号码和这个隐形型SIM卡号码在同一部手机中使用。

否则，追踪者可以通过两种方式找到您的身份：

- 一种方法是在电话网络中寻找可以关联号码的行为模式。

电信公司出于各种原因监控其网络中各种号码的行为。当您在同一部手机上切换到增强隐私的SIM卡时，他们可以知道您的SIM卡在同一位置离线后立即又上线了新的卡（反之亦然）。

随着这种模式的重复，电信公司可以通过查找在此新号码上线之前脱机的号码，来识别新的未知SIM。

这对电信公司来说并不难，因为他们一直在这么做。

- 另一种方法是跟踪手机的IMEI号码。

每部手机都配有IMEI号码。此号码可视为您手机的序列号。电信公司可以使用手机 IMEI 号码关联该手机上使用的所有SIM卡。

所有智能手机都有唯一标识符，应用程序开发人员可以使用此ID作为锚点来跟踪您的假名和真实身份之间的联系。

这可能是一个问题，取决于您使用新身份的应用程序以及您使用它们的方式/原因。

缓解措施

- 最好的方法是用现金购买一部全新的手机。

- 或者您能确保干净的二手手机。

- 在此手机上完全使用假身份，与真实身份彻底切断。

如果您无法获得隐私程度足够高的SIM卡，则可以使用虚拟号码。

[image]

返回：[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

以下是一些虚拟号码服务。

如果您使用虚拟号码来设置 Twilio，请谨慎选择，因为其中一些可能无法使用。

- Google 语音应用

请注意该帐户已连接到**Google**帐户。谷歌知道您是谁。而且他们会毫不犹豫地与政府间谍合作。并且对中国朋友来说，在地缘政治冲突下避险的可行性已经快速下降了。请斟酌。

- Burner：这是智能手机应用程序，Burner是另一种手机号码。

该应用程序可以拨打/接听电话和发送短信。使用美国或加拿大号码。

- CoverMe：类似Burner，但它声称保护您的消息，因此 CoverMe 的工作人员无法知道您是谁。

除虚拟号码外，该应用还包括一些其他工具和功能。

- Hushed：也类似Burner，且提供国际号码和电话。

并非所有号码都提供相同的功能。大多数都有短信和语音通话作为选项。

总之，您的个人威胁模型很重要 —— 因为那些寡头公司大多数时候

只受政府间谍的指使，所以，如果您的对手是政府，那么最好避免使用任何寡头公司的服务；如果您的对手是前女友/前老板/债主 ……那就不大一样了。

[image]

返回-可视化威胁模式练习：[image]S01E05-T4 态势监测和威胁清单

返回-防御策略制定练习：[image]S01E06-T2 找到弱点建设新的防御能力

第2步：获取与您的真实身份分离的电子邮件地址

创建新的在线角色的另一个重要步骤是拥有一个不会追溯到您本人的电子邮件地址 —— 一个“隐私增强型的电子邮件地址”。

无论您采用哪条路径来建立新的私人帐户，都会需要它。

[image]

返回-工具：[image]隐私型电邮提供商的列表

返回-工具：[image]临时电邮

返回-工具：[image]一些较安全的电邮客户端选项

返回-工具：[image]一些匿名的电邮选择

返回-工具：[image]Tor上的加密邮件服务

返回-工具：[image]临时/一次性电子邮件服务选项

重要准备：使用安全的 VPN

以下步骤涉及访问网页。强烈建议您使用Tor浏览器等隐私增强型浏览器访问这些网站。

如果您因为各种原因无法使用Tor，建议使用 Brave 浏览器，或者在’私密浏览’模式下使用 Firefox，并安装 Privacy Badger 和 Https Everywhere 扩展程序。不要使用Chrome！

[image]

在本站“工具”栏目中搜索“浏览器”，以找到安全的浏览器建议。

使用假名[image]假身份 和加密货币购买的VPN。

切勿使用任何在线支付渠道。

现在您可以继续在安全的电子邮件平台上创建电子邮件地址了。

第3步：设置 Twilio 号码以创建无法追踪的在线帐户

使用从步骤1获得的电话号码、以及从步骤2获得的电子邮件地址，您就可以使用 Twilio 创建任意数量的虚拟号码。

它是开发人员的技术工具，允许应用程序发送/接收大量文本。

与SIM卡和其他虚拟号码相比，Twilio 号码便宜且维护成本低。

您可以使用与您无关的信用卡或使用现金购买的 visa/master 礼品卡

购买帐户。

由于 Twilio 技术性稍强，本指南将概述如何创建帐户以及如何使用它来接收验证文本。

在 twilio.com 上创建一个帐户

进入 twilio.com 并点击“注册”，您将看到注册页面。

请记住，填写表格时不要提供任何个人身份信息。

您可以使用假名，以及步骤2中的隐私增强电子邮件地址。

[image]

点击“开始免费试用”按钮后，它会要求您通过电子邮件验证您的帐户。

[image]

由于 Twilio 提供免费试用而没有信用卡注册，因此他们使用电话号码作为验证帐户和限制注册的另一种方式。

在这里，您可以使用从步骤1获得的电话号码。

[image]

验证了电子邮件和电话号码之后，您就会进入下面这样的屏幕。现在点击‘SKIP TO DASHBOARD’。

[image]

登录 Twilio.com

此时，您将被要求使用您用于注册的电子邮件地址和密码登录 Twilio。

[image]

在 Twilio.com 上创建您的试用版号码

登录时，您应该能看到“获取试用号码”按钮，单击该按钮。

您可以继续“选择此号码”。（如果要搜索可用的试用号以找到您喜欢的号码，您还可以点击“搜索其他号码”）。

请记住，某些国家/地区在电话号码方面有严格的验证法规。出于本指南的目的，建议您选择美国号码（+1国家/地区代码）。

[image]

获得 Twilio 号码后，您可以使用它来接收您正在设置的服务的SMS验证码。

本指南使用的例子是创建一个 Telegram 帐户。

成功后您就可以运行一个相对安全的 telegram 频道了。

请务必记下您的 **Twilio** 号码，用户名和密码。建议您将它们存储在密码管理器中。

[image]

返回：[image]什么是凭据填充攻击？如何选择密码管理器？

还建议您在此 Twilio 帐户上设置2FA（双因素身份验证）；并且建议按照 Twilio 的指示使用 Authy 应用程序。

开始创建应用程序账户

Twilio 将向您发送一条消息，祝贺您成功创建了电话号码。您现在可以在应用程序上使用它了。

[image]

将试用版号码升级为付费帐户

对于接下来的步骤，您需要首先将 Twilio 帐户从试用版升级到付费帐户。

你可以创建一个最低20美元的账户。付款方式始终是信用卡。如果您想保持匿名，建议您使用现金购买的礼品卡。

这在某些地方比其他地方更容易。比如在美国，大多数药店（Walgreens，CVS等）和便利店（711，Family Dollar等）都提供礼品卡。

[image]

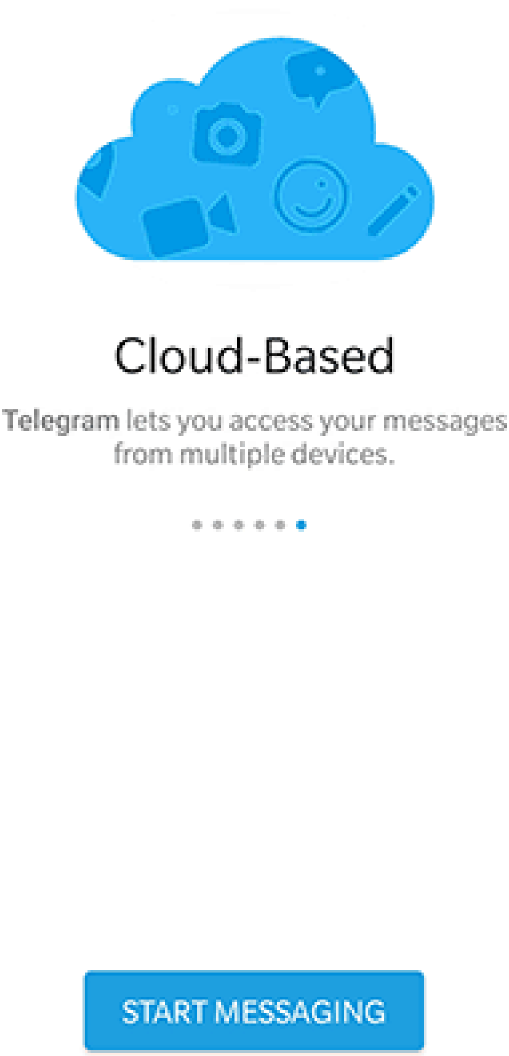
现在就可以开始使用您的Twilio号码和隐私增强电子邮件来创建无法透露您真实身份的在线帐户了。

使用 **Twilio** 号码启动 **Telegram** 帐户

在 Telegram（或其他应用程序或网站）进行设置。

在手机上安装应用程序（您可以返回步骤1获取有关手机设备的详细提示）。

这里只是案例；相同的步骤适用于 Signal，Whatsapp 等。



Telegram 会要求您输入您的号码以接收验证码。输入您的 Twilio 号

码。

[image]

检查 Twilio 以获取验证码。

您需要知道在 Twilio 中如何找到要输入的验证码。

[image]

登录您的 Twilio 帐户。

[image]

单击位于中心的三个点的cirlce（...）这将带您进入“所有产品和服务”选项。

[image]

需要访问 API EXPLORER，它允许您查看流入或流出 Twilio 帐户的数据，而无需编写任何代码。

[image]

在 API EXPLORER 中，单击“Programmable Voice”下拉菜单，将其更改为“PROGRAMMABLE SMS”。

[image]

现在您正在查看与 PROGRAMMABLE SMS 有关的所有API端点。

单击 MESSAGES 以显示与 MESSAGES 有关的所有API端点的列表。

执行此操作时，您应该看到 POST，DELETE，GET 操作的列表。创建消息，删除消息，查看消息，查看消息列表，修改消息等。

[image]

点击“View a Message”，这样您就可以打开并看到验证码。

在红色按钮“Make a Request”上方是一个名为消息SID的下拉列表。

您收到的 Twilio 号码的每条短信都应该有一个SID，以从新到旧的顺序列出。

应该有一个’Hello From Twilio’SID。一旦您想要的SID显示在此框中，请单击红色按钮。

[image]

默认情况下，数据的格式是人类可读的。可以清楚地看到一条消息。RESPONSE 的第一行是：

好啦，验证码是 48560；现在只需将其输入 telegram 应用程序即可！

[image]

最后再次提醒，**telegram** 并不是被推荐的通信工具，而且其频道功能不加密。这里只是一个创建假身份的演示，您可以使用相同的步骤创建对您来说足够安全的应用程序账户。

[image]

返回：[image]Telegram的隐私保护指南，和信息搜索工具

[image]
[image]

清扫和清点-信息篡改的重要步骤：完美隐身 S04E05

[image] 关键词	清理 自检 逃亡
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月6日
[image] **Description**	心理安全；行动安全性

任何人都应该了解这些知识 —— 如果您真的明白信息的昂贵价值，会格外重视它们。

- Table of Contents

1、钱包和口袋
2、钥匙链或者其他免费小商品
3、客厅
4、家庭医药箱
5、车库
6、卧室
7、厨房
8、书房
最后

E03 中列出了隐身思考方式的三步策略：信息篡改、信息杜撰、信息重组；并讲述了第一部分内容的概念。

现在我们进入第二步的准备工作。

[image]

您需要在这个过程中尽可能保持冷静 —— 很多尝试隐身的人由于紧迫的情况而处于慌乱之中，也因此很多平日里熟知的技巧都想不起来了。这是极大的悲剧。

不管做任何事，心理素质都是需要强调的硬项；恶意行为者（包括追踪者）最擅长的就是挑战目标人的心理自助能力，以刺激其慌乱，从而导致其疏忽、并自动做出愚蠢的决策。

抵制方案就是加强自己的冷静。情绪管理 ，这在平时需要一些练习。

在信息篡改之前，您必须认真思考信息可能隐藏的每一个地方 —— 不论是现实中还是数字世界里，都是如此。

[image]

从“威胁知识库”进入相关镇压手段：[image]隐蔽性地突袭住所 、和 抄家

使用对抗性思考方式，把自己想像成追踪者，对自己的一切进行侦查。列一个清单，然后逐一处理。

乍看下似乎是一个庞大的工作，但是这里面也可以有技巧，以逻辑简化工作量。

[image]

在数字世界中筛查自己的信息：[image]自我人肉

接下来我们从现实中的筛查开始。

重点先关于以下这些部分 —— 这是大多数人最容易留下痕迹的部分。

1、钱包和口袋

拿出您的钱包看一下里面装了哪些卡。

每张卡（任何卡）上都有大量的个人信息，甚至信息量叹为观止。

除了基本的联系方式信息和交易记录之外，部分卡上可能还有奖励计划。

如果您有常旅客里程数、优惠出租车服务、或者连锁酒店积分等等，可以想像，一旦追踪者找到这些无疑是找到了一座金矿；尤其是当您用里程数换了机票飞往了新生活时…… 您可能就没有新生活了。

此外，您有百货店的奖励卡吗？常客卡呢？这些商店是否有您的真实姓名和联系方式？

如果您的身上还有一部智能手机或iPod，苹果/安卓账户会揭示多少关于您的个人信息？您是否还有其他在线商店的账户？订餐？网购？网约车？共享自行车？……

一切都是导火索，都需要清除和篡改。最好是 从平日就注意这些细节。

2、钥匙链或者其他免费小商品

继续思考。药店掌握多少关于您的信息？杂货店呢？健身房呢？或者公交卡？您是否购买什么东西被动加入过某个公司的群发邮件列表？或者因为参加过其他促销活动而获得了一个免费的钥匙链或者其他很垃圾的小商品？

继续问自己：谁有备用钥匙？是否曾经把钥匙交给生命中任何一个重要的人、朋友、或者保洁阿姨？如果已经与此人断绝了关系，您是否要回了钥匙？能保证此人没有私下另配一把新的钥匙吗？

立即换锁才是完美选择。不会建议您对亲密关系也保持怀疑，但是要知道，人是会变的（这也是人类最大的神秘魅力之一），并且您不可能预测到变化的准确时间。于是，留一手会有好处。

[image]

3、客厅

到客厅去看看。如果有电视、音响、空调、以及其他设备，那么一定会有保修单。保修单上都印了哪些内容？生产商/销售商手里是否有您的现住址和手机号码？

如果某些电器是别人送的，那么生产商手里掌握的究竟是送您东西的人的信息，还是您的信息？

无论是哪种情况，保修单对于追踪者来说都是巨大的优势；哪怕找不到您本人的联系方式，也会能找到至少一位您的老朋友或家人的联系方式，于是就可以通过社交工程战术从他们那里套出您的信息。

继续。沙发、长椅、柜子等等这些家具，是否都有保修单？如果追踪者冒充您的身份找到了那些商家，他们能从商家那里套出哪些信息？

所有这一切东西都是如何支付费用的？是信用卡还是通过商店的账户？

任何一个聪明的追踪者只要嗅到您的任何一丝气息，就一定会努力利用它。

他们会找到当初您购物时的家具店、地毯店或者是品牌经销处；他会与这些商店联系，冒充您的身份，就说单人沙发或者任何一件您买过的东西的保修单找不到了。不出5分钟，他就会能拿到地址和电话号码。

而且这种利用保修单和签帐卡的社交工程方法甚至可以实现跨国追

踪。

[image]

从“威胁知识库”进入相关主题 🌎跨国维稳

4、家庭医药箱

药箱里可能充斥着大量私人信息；药品标签说明了您的健康状况，药单上还有给您看病的医生和药房的名字。

药房有您的医疗保险记录，医疗保险公司会把您的所有开药情况详细记录下来。

尤其是，如果您是一个政客或公众人物，您肯定不想让任何人知道您在使用赞诺安或百忧解（镇静剂和抗抑郁药物），伟哥呢，也一样吧？

但是想要加害您的人会想方设法查出这些信息。它们可以非常致命。

您平时把这些东西放在哪？卫生间里吗？有谁借用过您的卫生间吗？最好是不要把上述物品放在触手可及的地方。

5、车库

车库一样是追踪者的天堂。

人们会放置很多机器和工具在车库里，还有早已被遗忘的垃圾中都能找到关于您的线索。

不论是割草机、电动钻头还是什么工具，上面一般都会有序列号，而且序列号是贴在保修单和购物单上的。保修单又附在购物单之后，上

面一般会有您的姓名、地址、电话号码，以及您所提供的一切信息。满满的，都是情报。

移除所有这些东西上的序列号，在扔掉和卖掉这些东西之前。

大多数人在整理“垃圾”的时候只是想着“我是否还用得到”的问题，而不是：“追踪者能用它们来做些什么”。

这种思考方式肯定不是被支持的，它很危险。尤其是当您正在准备逃难的情况下。

我们会建议您在日常整理垃圾的过程中也能保持*安全的思考方式*——— 多想想自己扔掉或卖掉的东西对于恶意行为者来说意味着什么。

不要简单地把废旧物品塞进垃圾袋，最可靠的方法是，烧掉它们。

[image]

6、卧室

大家都知道不雅视频是什么，所以卧室必须是私密空间。

平日就不要在卧室里放置任何带有摄像头和麦克风的设备，比如手机、电脑、家用摄像头、所谓的智能某某某等，如果习惯于在床上看手机/电脑，用黑胶布贴住摄像头。

任何可以用来威胁和勒索您的东西，都是您最大的 弱点 。

7、厨房

和客厅一样，厨房里也会有一大堆带有保修单的东西：冰箱、微波

炉、洗碗机、炉灶 …… 甚至食品也存在能指向您的线索。

食物是从哪买的？您是否参与过团购、聚划算之类的活动？几乎所有商店都有“认同卡”，只要扫一扫就可以享受当周的优惠价格 —— 这些商店把您的地址和电话都存档了，有些甚至还会有您的支付账户信息。

当然他们都知道您买了什么、在哪买的、什么时候买的……为什么要把这些真实信息提供给那些人？

喜欢美食吗？订阅过美食杂志吗？是否在特色美食公司邮购过食品？聪明的追踪者就会利用这些信息找到您的下落。

如果追踪您的人知道您喜欢吃什么 —— 您在社交网络上晒的美食照片中哪种食品的出镜率最高 —— 追踪者就可以瞄准提供此种食品的所有公司，一一给这些公司打电话，声称他就是您“这个老客户”，要求订购，并声称送货地址已变更。

很简单就能套出您被登记过的旧地址甚至私密联系方式。

可以肯定的说，绝大多数人并不会以为自己在社交媒体上晒美食这件事有多大的危险性，当然，很多时候它不危险，但是，如果有人暗中针对您，这些美食就是您的枷锁。

还记得上一集中麦当娜的粉丝如何被抓到的例子吗？—— 没错，您的任何偏好、兴趣、口味、心理特征，都是追踪者的盛宴。

最好平日就注意这点：不要让任何人尤其是不怎么可靠的人了解您。尤其是不要把真实的自己放在互联网那种地方上。

8、书房

电子设备、以及放置电子设备的地方，对于追踪者来说很容易形成突破口。

您的IP地址以及硬盘上没能清理干净的信息，会告诉侵入者或骇客能找到您或者盗用那您的身份所需要的一切。

如果追踪者通过上述任何一种方法找到了您的旧址，闯入您的房子，他们就可以拿到您的电子设备，以及您家里未受保护的无线网络传输信息，用不了多久就能找到您的下落 —— 您要去什么地方、到了那里之后计划做什么。

[image]

返回 - 工具：[image]定期清理硬盘

返回 - 工具：[image]彻底卸载

公共场所的不安全无线网络连接反而难以追踪。因为在任何一个时间点，都会有至少数十人同时在使用这一网络；要确定某个具体的使用者是极为困难的，除非追踪者确切知道目标的IP地址。）

Tails 是个好办法。斯诺登就是用这个方法帮助自己抢夺时间的：

[image]
[image]

返回：[image]他们如何抓捕说真话的人？灾难和教训

不仅是电脑手机，打印机和扫描仪一样很危险。

您知道打印机的用户识别号码是什么东西吗？这个号码会告诉人们这张纸是从哪一台打印机上输出来的。制造商对此几乎没有做过任何宣传，但这个东西就是追踪的重要线索。

此外大多数人会把账单和文件放在书房的电脑旁。在您准备隐身前肯定会想到把这些东西扔进碎纸机，但是，千万别把碎片直接扔进垃圾桶，因为很多碎纸机都太粗糙了，想要找到您的人会有的是时间把它们重新拼凑起来。

所以，烧掉那些碎片，或者把它们扔进下水道。

此外水电公司是最大的危机，它们的安全级别很低，于是更危险。如果您依旧决定住在原地，需要想到一些可行的方法将关于您的信息篡改为难以被追踪者识别。

这是下一步工作。

[image]

最后

以上针对的是大多数人的习惯。梳理它们的目的主要是强调一种思考方式 —— 如果您有比较个人化的收纳习惯，您应该能使用同样的思考方式，针对自己的习惯进行筛查。

完成这一切后您就可以继续下一步了。

如果您想要知道自己是否彻底完成了清扫追踪线索的工作，您可以自己聘请一位私家侦探来追踪您。以此检验您的隐身质量。这就像是网络安全措施中的渗透测试。

但不要使用任何在线支付的方法和任何银行卡支付，用现金；最好能选一个离您比较远的私人侦探。

把名字给他们，附加一些基本的信息，比如旧地址、电话号码等，看他们能挖出多少东西。那些人是只认识钱的，他们一般不关心是谁在聘请他们以及什么目的。

一旦他们挖出任何蛛丝马迹，您应该立即补上漏洞。到此才能称为一切就绪。

下面应该开始第二步工作了：信息杜撰。

重复强调这句话：人们之所以会陷入无法扭转的危机，是因为一个广泛的心理弱点 —— 总是认为最糟糕的事不会发生在自己身上。这是大脑的防御机制；但它也非常危险。

没有人能预测危机，所以聪明的人应该知道如何在平日里保护自己。就像您会下意识地离家前锁门、将干燥的纸张远离火源那样。

[image]
[image]

令人兴奋的心理过招：完美隐身S04E06

[image] 关键词	匿名购买 心理战 手机号 电邮 社交工程 移动设备 逃亡
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月7日
[image] **Description**	心理安全；行动安全性

狡猾并不总是个贬义词。尤其是当它用在正确的战略性意义上时。

- Table of Contents

  1、鱼钩
  2、鱼线
  3、鱼饵
  1、储值卡
  2、预付费手机和电话卡
  3、虚拟电话号码
  4、包裹投递点
  5、电脑、电子邮件和邮箱地址
  6、其他工具
  7、记住紧跟时代

开始下一步策略：信息杜撰。它能把您的聪明才智发挥到极致。

[image]

到目前为止您已经完成了信息篡改；也已经梳理了所有外在信息，并

做到了掩人耳目。

现在，您要做的就是设置一系列虚假的线索，去误导追踪您的人，使其寻找您的过程困难重重。就像《最危险的猎物》中雷斯福德的做法。

此时您应该有两大目标：

> 扰乱追踪者的视线，让他们在错误的地方瞎忙；尽可能将您的个人资料变得极为复杂、极难获得，并且在展开解谜的过程中，让追踪者不断遭受挫折。

人们在打点行李准备上路之时，一个最常见的、生死攸关的错误就是——压根没想到应该让追踪者忙起来。

如果只留下了一条线索，哪怕您费尽心机极力掩饰，也同样会让追踪者有机可乘。他们可以彻底调查这一线索。

别便宜了他们。

追踪者将是您见过的最富有行动力和想象力的人；只要线索正确，他们肯定会能挖出您。

所以，您要做的就是， 让线索不正确 。

这就是为什么杜撰消息非常重要——追踪者如果掌握了主动权，他们毫无疑问会玩死你；而如果您能抢占主动权，就可以玩死他们。

您需要3个要素：鱼钩、鱼线、鱼饵。

[image]

返回：[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基

础课 S06E06A

[image]

1、鱼钩

鱼钩就是您故意布下的一条线索 —— 它是假的，其目的在于让追踪者发现。

它不仅要逼真，而且要能够让追踪者在发现时兴奋不已。

还记得《La casa de papel》中“教授”如何布局培训楼的情节吗？——遍地都是行动计划路线图、指纹、以及各种追踪线索，并且，让警方在费尽心机的情况下才发现了这一“宝藏”。

然而一切都是假象，只为了绊住警方的脚，一切都是有意布下的局，只为了拖延时间让行动者顺利脱身。这就是鱼钩。

在信息篡改中，鱼钩可以是：比如，故意地申请房贷、故意租房、或者办理信用卡，以此误导追踪者对您的征信状况进行调查。

您可以做任何事 —— 请注意，最好能事先推测到追踪者最容易上什么当（或者说他们习惯于从哪里开始展开调查），然后就您可以抢在前面在这些路径上挖坑了。

比如，您明知道追踪者会监听您的电话，那就用这部电话给他们放烟雾弹 —— 这一做法也在《La casa de papel》中有充分呈现，行动者将警方植入Rio身体的监听器变成了操纵警方的便捷武器。

📌

还是那句话，知己知彼，很重要。您和您的对手谁先摸清了对方的思维方式，谁就能取得胜利。和下棋的道理一样。

2、鱼线

您留下的假线索越多、越乱，对手就会越多眩晕，他们越是专注，死得就越快。

每一条线索上都让它布满疑点，疑点是最好的引擎，追踪者会格外好奇每一个无法解开的谜。他们会想要知道答案，他们就会去研究、去实地考证，这就会消耗他们大笔的金钱和精力。

更快速地接近枯竭。

不要让他们轻易得到这些线索。

没有人会重视那些自己能够轻易得到的东西，就如您所知道的那样，这也体现在追踪者身上 —— 您需要做的就如下棋，在3步之外等着他。看着他踏遍所有您布置好的泥坑。

就算您得罪的人是政府情报机构也一样。除非您是重大通缉犯，否则政府不会有无穷无尽的预算等着被消耗。

时间是这场游戏中最值钱的东西。

3、鱼饵

当权者都喜欢全面掌控，肯定会第一时间追查银行卡和在线支付的使用；那就在这里下鱼饵给他们。

比如申请一张借记卡，然后交给那种满世界飞的出差狂人；然后追踪者就会发现“您”正在全世界飞奔。

📌

这就是鱼饵的思考方式：让它看起来有线索，其实千头万绪，就算是专业侦查团队也需要花费几年的时间才能理清头绪。

追踪者会想尽一切方法获取您的电话通话记录，然后他们就会发现银行的电话号码，就会知道您的钱走向了哪里。

此时他们就很可能冒充您本人，给那些银行打电话，以骗取更多的信息 —— 接下来他们就会发现一个活跃的账户。

他们就会感觉到“大功告成”的喜悦 —— 但事实是，他们再一次被套牢了。

看着追踪者的晕头转向，您可以充分体验自己的杰作。

[image]

创造力非常重要。

不论您准备加入的是哪一种斗争，创造力都是您最强大的武器。

接下来介绍一些您可能用得到的武器。肯定不完整，但它们会比较顺手。

1、储值卡

去附近的便利店或沃尔玛挑一张储值卡。

请用储值卡、礼品卡、现金购买任何东西，必须停止使用信用卡和在线支付。因为要提取信用卡记录实在是太容易了。

礼品卡最大的优点就在于，完全不会有记录。

2、预付费手机和电话卡

如果有任何人认识您本人并同时知道您的手机号，这张手机卡您就不能再使用了。

[image]

您的旧手机也该彻底丢弃，它是您最大的致命弱点之一。但是千万不要简单地扔掉，最好能把它砸成碎片，并扔进多个不同的公共垃圾箱里。

在这点上千万别偷懒。用现金购买预付费手机，尽可能不要泄露任何个人信息。如果卖家必须请你注册，就假装写错名字，或者写得潦草一点。充值时用现金。

这会比普通的手机和座机更安全一些，尽管并非万无一失；如果您提供的是不准确的名字，他们就很难追踪到您。

此外其余的一切都是可以追踪的，比如您拨出的电话以及拨打电话的大致区域。如果追踪您的是政府当局，做到这点就会更容易。

所以，万无一失的方法是，不使用任何通信设备。

[image]

从"威胁矩阵"对应的主题进入 [image]数字技术限制和最佳实践

如果必须使用，请仔细阅读用户指南，了解如何设置呼叫转移。重要通话结束后彻底毁掉这部手机。

在本机上删除通话记录很容易，但仅仅是从您自己的手机上删除了，电话公司仍保存了这些记录，追踪者仍然可以找到这些记录。这就是为什么必须打电话时，您应该勤换手机。这非常重要。

讲一个真实的案例。一个叫马修的人假装在一条河里溺水淹死了，然后逃到了邻国。他使用的策略就很聪明。

他把自己的黑莓手机扔在了加油站，怀疑他还活着的追踪者查看了他的手机记录，通过这些记录，追踪者找到的其实是街上一个流浪汉。

如果这是一部注册在您名下的手机，这个方法是无效的。

3、虚拟电话号码

如果不方便购买预付费手机，不含实际位置的虚拟电话号码也是个好办法。方法在E04中。

操作安全很重要！不论您使用任何安全技术都是如此。

JConnect 也是个好办法，不仅可以发送语音邮件，还可以在 efax.com 上接收传真。这些号码都很好用，可以线上组建，非常迅速，您能够买到世界各地的号码。

想让追踪者认为您在巴黎吗？购买一个归属地为巴黎的电话号码，通过巧妙的方式泄漏给追踪者，就可以了。

[image]

4、包裹投递点

如果您不想被人知道您的住处和去向，就需要至少一个匿名的投递点来接受邮包。

事实上您需要的投递点远不止一个。

思考方式就如多个预付费手机一样，最好的方法是，创建一个含有多

个投递点的复杂系统。

这样一来，盯上您的追踪者即便获得了您的记录，也解不开其中的谜团。

不要开设邮政信箱。任何一个国家的邮政总局都是最容易获取信息的地方，追查您的下落非常容易。

您甚至可以在储值卡中留点钱，找一个热闹的超市、一辆公交车或者其他人多的地方，假装丢落。捡到这张卡的陌生人会在别的地方使用它，这就自动形成了一个新的假线索。

不过请注意，记得要擦掉卡上的 [image] 指纹 。

在填写任何申请表的时候，潦草的字迹也会有帮助，比如把1写得像7，把4写得像9，以及包含错别字，就算是您布下的诱饵，这样的处理方式也能让追踪者揪头发。 BACK 笔迹分析

5、电脑、电子邮件和邮箱地址

如果有能力的话建议买一台新电脑。但是继续使用旧电脑和家庭网络来完成一些无关安全的事。这样一来，任何发现您的IP地址或侵入您的电脑的人都会认为他已经找到了您。

用家庭网络随机查看一下外国的目的地和公寓楼，这些都是制造假线索的好办法，把追踪者引入歧途。他们只有挖到最底部才能发现是死胡同，这就为您争取到了很多时间。

买来的新电脑千万不要直接连接家庭网络。也不要在[image]藏匿点或安全屋 中使用。如果是在中国内地的朋友使用Tor比较困难的情况下，建议去个离您的住处比较远的地方，找一个公共无线网络。哪怕您只是想看一眼猫咪的照片，也要这样做。

关键在于，您的目标应该是：不要让任何人把您的名字和这个IP地址联系起来。

如果您不得不使用网吧处理一些琐事，要注意网吧里面的摄像头，要确保它们不会拍到您的脸（面部识别）。千万不要在网吧里打印任何东西，因为公共打印机会记录下您打印的内容和时间。

[image]

返回-一个演示：[image]与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧

最好能使用异国的电子邮箱，比如您在中国，使用法国的邮箱；并且邮箱名字不要与您发生任何关系，比如您是众所周知的摩托车迷，就不要使用诸如“哈雷15”这样的名字。

总之，竭尽全力不要暴露任何关于自己的线索，要让任何人看到这个邮箱时也想不到是您。

不用担心有人会通过不安全的无线网络获取您的信用卡和身份证号，因为您绝对不会在网上公布任何一点点个人身份信息。

如果您想买书学习，那就用现金买，千万不要使用任何在线支付渠道。

6、其他工具

除了上面这些之外您还需要些什么？这取决于您想在哪里生活、做什么、如何谋生。

下面这些东西都能有所帮助（并非所有国家都能顺利找到这些东西，选择在您的国家相对可行的类似方法即可。这里的重点是思路而不是工具）：

- 来电身份伪装卡/APP：它可以改变您的号码在对方手机上的显

示方式。

- 开脱服务：类似 alibinetwork 那种，同类的还有很多。可提供由旅行社、酒店、研讨会和“雇主”提供的假的不在场证明。约会进展不顺利时他们还可以提供假的“救援电话”。（顺便说这是个不错的业务）

- 保守型语音信箱服务：允许您登陆和发送语音邮件，邮件直接进入对方的邮箱，没有电话提醒。

- 一次性电邮地址：BACK 在本站“工具”专题中搜索 “电邮”，以选择适合您的安全解决方案。

- “自由手机”：没有身份信息、没有任何官僚主义的麻烦、支持比特币购买。但是小贵（当然 Purism 也一样），在本系列的背景下，用户需要权衡是钱重要还是命重要。

IYP的项目完全独立，与任何商业和政治机构都没有关系。所以我们不会推荐产品。您可以用安全的方法搜索“**Secure Smartphones**”、“**Encrypted Phones**”，查找相关品牌。

7、记住紧跟时代

科技每时每刻都在进步，政策也在改变；所以您必须紧跟这一进度，在出现新的跟踪监视技术/手段和安检政策时及时考虑添加新的策略。

[image]

返回 - 战术性局势利用是安全训练中的一环：[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局

要知道，最新的技术不会很快投入使用，更不会很快变得高效；人力监视在近几年内都将作为技术监视的必需搭配。

于是，把重点发在搞定人心上比不断遭受新技术惊吓，要实际得多。

尤其是，请记得：监视是一个持续不断的过程；随着时间的推移它对您的危险程度会不断加深 —— 因为它了解您更多了。

所以，不要指望在短时间内迅速实现全面隐藏自己。您应该在平日里就多加防备，让自己熟悉 [image] 数字技术限制和最佳实践 ，熟悉防御的思考方式，这样才能在需要的时候快速实现一步到位。这就像攒钱—— 就算您现在什么都没打算买，也应该节俭以保证有足够的积蓄，这样才能应对不时之需。

[image]
[image]

用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

[image] 关键词	个人 反监视 对抗性思考方式 逃亡
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]假身份 ；分身 ；[image]反监视
[image] 创建时间	2025年2月8日 12:00 (GMT+8)
[image] Description	行动安全性；心理安全

不论是秘密警察、特工、便衣、私人侦探、还是任何恶意的偷窥者，他们都有一套观察记录的方法。

- Table of Contents

  要找什么
  找到有价值的细节
  为什么这一技能是重要的？
  注意文化习惯
  肢体语言
  实践观察

[image]

在东京的时候，我遇到了一位名叫 Danny 的以色列人，他在那段时间里成了我最亲密的朋友。在年轻时代，Danny 就已经成为了一个非常成功的企业家。他也非常喜欢亚洲的艺术和文化，也是这，最终将他带到了东京，在我到达之前他已经在那里生活了近十年。

Danny 是一位自学成才白手起家的百万富翁，而且是一位天生的商人，世界旅行家，艺术史专家，美食和高端烈酒的鉴赏家，以及五六种语言的流利演讲者。作为一个引人入胜的家伙，他现在仍然是一个真实存在的“世界上最有趣的人”。

在 Danny 教给我的许多事情中，令我记忆最为持久的和最有用的一点就是，关于识人的艺术—— 如何读懂一个人，如何理解隐藏在微妙表达背后的真实意图，如何理解有意识的和潜意识的习惯，以及如何使用这种类型的知识以获得各种优势。

要想达到这种能力必须从内心的自我反思开始。换句话说，理解其他人将建立在理解自己之上，控制自己的弱点、肢体语言、细致入微的表达和情绪状态。

我们会出门去练习读人和人际影响技能，主要是在东京高档社区—他们的咖啡馆，餐馆和俱乐部都很时髦。这就像是一场开放式的国际象棋游戏，你可以小心翼翼地定位自己，并在你玩的过程中尝试计算接下来的几步。然后，我们将评估事情的进展，讨论哪些有效，哪些无效。

但当我后来来到以色列，在日本学到的东西开始遭受到打击。人们都是一样的人，无论他们住在哪里，但文化对于人们如何表达自己有着至关重要的影响。谈到日本文化，特别是在高端圈子里，人们非常保守，欲望传达得非常巧妙，真实意图隐藏在厚重的客套和礼貌之后。就像你在中国经常能遇到的那样—每个字的中文都能听懂，但其本意很可能不是你理解的那样。

相比之下，美国人、以色列人等处于这一范围的另一极端。几个月忙着习惯阅读日本人行为的微妙之处让我在抵达以色列时感到几乎能透视了。这里的人看起来很幼稚，即使他们试图避免显露这点。每个人的情绪状态、欲望、动机和行动，犹如画卷一般在视线中展开。看到某人时就给你一种似乎在偷窥什么的感觉。

当时我并没有想到这种技能在我的职业生涯的未来会变得非常有用。能够阅读他人—推断和诱导他们的各种事—对于保护和现场情报操作

来说非常有用。

所以，我现在可以给你一个速成教程，并分享一些其中的秘密。

要找什么

当涉及到读人时，你应该“相信”你的直觉。别误会，相信你的直觉并不是一个错误，但绝对不是每个人的本能都能迅速发展，即使是那些本能更好的人，也总是有改进的余地。

是的，永远相信你的直觉，但绝不要止步于此。本能没有任何神奇或不可触碰的地方 —— 对他人的感知是由你在潜意识层面上感受到的混合接收信息所引起的。只是你对这种感知的意识比对潜意识的由来更清楚一些，这就是为什么一个本能感觉更像是一种原因而不是一个结论。

但是，不要将本能视为一种神奇的第六感，你实际上可以找到引发这些本能的根本性原因。通过将这些微妙的感官摄入从潜意识领域中带出来，可以帮你提高侦测技能并培养更好的直觉。例如，你是否看到一个看起来完全正常且不可疑的人？—— 这是第一印象。那么很好，问问自己究竟是什么让那个人给了你那种感觉。你有没有看到一个让你感到奇怪可疑的人？好，现在问自己同样的问题。

寻找这些本能背后的根本原因，因为它们确实就存在于那里。这是提高意识能力的好办法，帮助你了解人们如何以及为什么以他们的方式行事。

尝试检测、评估和理解尽可能多的细节，并试图弄清楚你对这些人的感受背后的“缘由”因素。你并不总是能够做到正确，但通过练习，你肯定会做得越来越好。

[image]

找到有价值的细节

在衡量外观时，我们想要评估和分析的因素一定要是人们可选择的因素。切勿将不可选择的因素（如种族、年龄和性别）等引入分析，那会非常糟，也要留心自己下意识的想法可能产生的误导。

例如，中文里有一句话叫“丑人多作怪”，这就是完全错误的逻辑。种族貌相这些问题不仅是道德问题，而且是逻辑问题，如果你试图根据一个人无法控制的非选择性、无意识的特征去推断关乎意图的结论，那绝对会失败。这种类型的分析不仅会导致假阳性设定，而且 ——尤其是—当它导致假阴性设定时，可能会非常危险。

幸运的是，可选择性因素包含在一个人外表的可被观察到的大部分细节中 —— 从头发到鞋子，以及他们可能穿着、携带、喜好或专注的任何其他东西。那个创造了“你无法通过封面评判一本书”这句话的人，不一定是在谈论书本身，只要你能注意细节并正确分析那些细节，它们就能告诉你很多东西。

几乎没有什么东西是随机存在的，一个人选择佩戴、携带或想拥有的内容可以告诉你至少以下两个重要事项：

- 这个人来自哪里？—— 他的背景、品味和资源。比方说经常穿着战术靴的人是什么样的人？什么样的人带着昂贵的 Gucci 手提包？为什么一个人要携带一个大型的健身包？这些事情都是有原因的，它们都与先前的选择有关。

- 此人会去哪里？他们为何选择在此时来到这个地方，并在之前选择穿着、携带或涂抹那些你刚才注意到的东西？他们的动机可能意味着什么？—— 例如，穿着军靴的人和穿着人字拖的人之间的动机可能有什么不同？在温暖的日子穿着一件明显很厚重的夹克的人，正在准备去做什么？考虑携带健身包的人来自哪里很有意思，但更重要的是为什么他们现在正试图将它带到此地？他们未来的意图会是什么？

我养成了一个很独特的习惯，就是观察人。我能在一大群等地铁的人

群中通过观察他们的外观和表情大致猜到他们各是做哪类工作的，正在急着去干什么。我曾经与人打赌，选中其中一个目标对象，我会事先写下我推测出的结论，然后尾随目标人，以验证对方的去向在我的结论之内。而且我经常能赢得这个游戏。

并不是说要你通过一个人的外表就准确推测其背景和意图，当然不是，许多看似可疑的指标结果显示完全无害（如果不是有点奇怪的话）。但是，你注意这些东西越多，你的感知能力就会越准确。你对线索提出的问题越多，你找出答案的机会就越大。

这可能听起来像是一些抽象的叙述，但是，通过一些练习，大多数人都可以非常快速地观察、思考、提问和解答—几乎就像是，本能。

为什么这一技能是重要的？

只要你生活在这个世界上就免不了要与形形色色的人打交道，不论是工作、社交、娱乐、恋爱，还是公民社会对思想警察和一系列跟踪者的警惕和揭露、反对派群体对盟友的吸纳和联合，要想做到准确和有利，其根本性问题都是：识人的艺术。

并且，当你掌握了如何通过观察就能预测对方的行为，你就能知道自己应该如何做才能达成你预期中想让对方体会到的意图。这就是社交工程学的重点。是的本集内容依旧在社交工程学技术系列范围内，这一技术能力会涉及到诸如巧妙的伪装、在对方不知不觉中套到实话、在他人毫无防备的情况下把他们引导到你的目的上来……等等步骤，显然，读人是其中绝对的关键部分。

再次强调我们需要大家利用这些知识做正确的事，和那些接受过此类能力高端训练的思想警察和卧底线人过招，而不是用其欺负无辜的人。

我们反驳过异议群体内流行的“抓特务”活动，因为这会导致原本就缺乏信任的一群人更加难以联合，打散这一群体恰恰是维稳的最有效目标之一。但是，必须承认，线人很可能是存在的，如何识别他们？如

何预测他们下一步会对我们做什么？社交工程学就是必需。

如果你想防止被骗、保护自己的资产和公司的安全，社交工程学也是必需的，还是那句流行语：要像骇客一样思考。只有当你能推测出对手准备怎么做的时候，才能在他们真的下手之前令其阴谋失效。

好的我们继续。

注意文化习惯

就如文章开头提到的，美国人、以色列人和日本人有着不同的习惯，这不仅表现在言谈举止上，也表现在穿着打扮和使用习惯上。举个例子，比如大号的健身包。在所谓的反恐时代，监视者对这种包的警惕性会非常高，一个背着大健身包出入聚会场合或中央级设置的人会令人紧张—— 这里面是不是炸弹啊？还是AK47？不不，这要看它具体发生在什么地方了。

在旧金山，你经常能在公共场所甚至公司晚宴上发现有人背着这种大号健身包出没。当然，这些人得到了检查和询问，结果显示基本没有任何安全隐患。旧金山的人，尤其是男人喜欢下班后去健身房，然后当他们去参加晚会时，不想把他们的包放在车上。这是一个完全无害的原因（除了有点占地方之外.....），但对你的练习来说，这仍然是一个值得观察的细节：可以告诉你这个人来自哪里、以及为什么他们此时将这个东西带到这个地方。

仅仅因为某些东西是无害的并不意味着你的观察技能和选择性分析不适用。

在与相关人员足够接近的情况下，会出现一个比较重要的侧面细节：就是香味。这可能听起来很有趣，甚至有点令人毛骨悚然，但它真的很具参考性。如果他们闻起来有点汗味的话，你前去搭讪的最好开篇应该是什么？如果一个人的头发有点湿，你能闻到肥皂或洗发水的味道，你能想到什么？…… 注意人们在早上上班时的气味，以及他们在漫长的一天之后散发的气味，这是不同的。谁的卫生条件差、谁一直

在喝酒或吸烟、谁使用过多的剃须膏或香水、是廉价的还是高档的？这将意味着很多有趣的背景细节。

嗅觉是经常处于潜意识水平的重要感官摄入之一。它值得被注意到。一些东西闻起来很奇怪的想法往往是非常直接的（比如不合适的场合，或者与衣着相貌所显示的背景不兼容）。您注意到的越多，您在检测人们来自何处、以及要去哪里、做出何种选择的机会就越大。

[image]

肢体语言

行为剖析是一个相当深刻的主题，但就我们的目的而言，并不一定要寻找微观表达或心理评估。相反，我们应该对形势的背景更感兴趣——这是哪里、正在发生什么，以及人们如何与这些因素相关。

首先，在你熟悉人们通常的行为方式之前，你不会在评估肢体语言方面处于非常有利的位置—— 忘了那些市面上的杂书吧，它们教了你很多错误的东西。在这方面，每个环境都是不同的，即使是一天中的不同时间也会有所不同，因此为“正常”或非敌对行为建立基线非常重要。这并不总是那么明确的，你将不得不接受各种各样的行为。但请记住，您看到的 99% 的人是非敌对的，因此可以为您提供该基线。

请记住，我们不仅仅关注一般人; 我们正在研究人们在特定地点、时间和背景下的行为方式。人们如何表现？他们的行为是否与这个地方和时间的大多数人的行为协调？一个人是否紧张地独自出现在这里，而大多数出现在这里的人似乎很开心？是否有人一起出现然后又分手？他们这样做的原因可能是什么？问这些问题是因为原因总是存在的。

在某些区域的访问受到监管的情况下，大多数人只是自顾自的走过去，好像安全对他们来说并不是一个威慑因素似的。一个非敌对的人可能正在考虑自己为什么要去某个地方，而不是考虑是否必须通过安全检查。这将表明他们如何行事。

具有敌意的人通常表现出不同的行为。

究竟是什么样的行为表明一个人有敌意，或者其他人试图隐藏某些东西？因为不同的人会表现出不同的行为模式，所以要确定这点是有点棘手的。例如，您可能会看到一个人快速行走，有一个明确的目标，全程表现为“隧道视觉”。相反，看到一个人走得很慢，紧张地环顾四周，时而停止并朝着目标迂回前进的情况也不少见。紧张和敌对意图可能以不同的方式表现出来，这一事实也许看起来有点令人困惑，但请记住，你并不是在寻找和分析的心理状态。

无论是太快还是太慢、隧道视觉、转向迂回，还是有什么东西，只要你意识到这不是大多数人在这种环境中普遍有的行动和行为方式，你就会发现需要对其加以更多的关注。

由于人类行为可能复杂多变，因此有许多看起来像特征的东西事实上是非常普遍的。

处于压力下的人几乎总是血液中具有更高水平的肾上腺素，于是就产生了一些可预测的结果。肾上腺素会增加一个人的血压，这往往会使人发热，有时会出汗。有些人的脸和耳朵可能会变红，而有些人可能会变得苍白—这两种情况都可能是坏消息。

高血压使人呼吸更快，使他们的嘴感觉干涸，导致他们尴尬地吞咽唾液，并且通常表现语焉不详。尽量注意人们专注于做的事。他们是否坐立不安、极度紧张、还是扣紧手指或抱臂？他们的眼神怎么样？是否完全避免过度接触或过度补偿？

再次，一旦意识到某些事情与大多数人在这种情况下的表现不一致，就会发现需要更多关注的东西。

实践观察

开发您的观察技能的一个巧妙的方法是，可以随时随地进行观察和评

估 —— 在街上，咖啡馆，火车上或在球赛期间。

如果你愿意，甚至现在就可以马上开始。停止阅读这篇文章片刻，看看自己身上有什么。你穿什么样的鞋子？（根据我的经验，鞋子可以告诉你很多关于一个人的信息）你的手指上有戒指吗？你的手机藏在口袋或钱包里，还是现在就在其他地方？你的手和指甲是什么样的，为什么会这样？你现在穿什么样的衣服，你有什么样的手表，手机套或眼镜？

所有这些线索，以及更多，都是在你到达此时此地之前所做出的选择。即使你当时没有给出太多有意识的想法，这些先前的选择也明显反映了关于你的某些事，它值得分析。或者假设一下，你收到了一些作为礼物的东西，你最下意识的动作是把它们还在哪？这将透露你对送礼物的那个人的觉知。

它基本上是一个福尔摩斯式的观察和归纳推理游戏 —— 或者我喜欢称之为“归纳观察”。你玩的越多，你就会越快熟练起来。继续推动和测试自己，看看你能够多快地检测到事物，你可以在尽可能短的时间内检测到多少细节，以及你对人们的背景和动机的评估是否正确。

[image]

如果您对某人的评估最终被证明是正确的，请记住它，并尝试查看它是否也适用于其他情况下的其他人。如果您的评估不正确，那也不坏—这意味着您正在尝试和学习。请继续。

最后，在将它们应用于其他任何人之前，永远不要忘记，使用您的归纳观察技能。注意自己的外表和肢体语言，并有意识地利用它们，以向外投射出适合您的情况的图像。这是给人们留下印象和塑造形象的好机会，所以，明智地使用它。

[image]
[image]

大清洗 - 扫荡危险区域：完美隐身 S04E07

[image]	关键词	分身 数字卫生 数字足迹 自检 逃亡 预防性
[image]	关联	[image]S04完美隐身-总章节：机智是重要实力
[image]	创建时间	2025年2月9日
[image]	**Description**	心理安全；行动安全性

残留物的致命性有可能很高。被您遗忘的任何残留，对于追踪者来说都是珍贵的大礼包 —— 别便宜了他们。

- Table of Contents

  1、找到它们
  2、关闭它们
  3、注意的问题
  1、电邮
  2、云服务
  3、数据碎屑
  4、查看服务条款中的数据处理政策
  5、移动设备相册
  6、讲卫生最安全

[image]

清洁和保持卫生，是每一个不想要被追踪、不想要被身份盗用和欺诈的人必需熟练使用的技能。

身份盗用和欺诈的风险比您想象中要大得多。

不论是在互联网上还是在现实中，一旦有其他人知道您的出生日期、住址、您的电话号码等等个人详细信息，就会导致您陷入严重的脆弱。

至少您应该能做到不要让那些身份欺诈者很容易操作 —— 不论您是不是想要实现完美隐身。

您正在使用强大且唯一的密码、您已经学会了识别网络钓鱼电子邮件的基本方法、并且您已经为每个帐户设置了双因素身份验证 …… 基本上，您正在处理个人网络安全101阶段。

但随着追踪者的深入新的威胁不断涌现，您可能正在寻找其他可以保护自己的步骤。

E04 最后一集将要介绍的是一个简单的防御方法：清理您的数字垃圾。

[image]

数字时代的人们很容易建立一大堆几乎未使用过的帐户，注册后很快就遗忘了。然而，这些帐户非常危险。您必须打扫干净。

您需要留意的东西包括：您从未跟进的免费试用、您已经放弃的流媒体服务、使用后发现并不是您想要的东西，等等。某些方面，这些旧帐户除了收集虚拟尘埃或偶尔发送电子邮件唠叨之外似乎没有任何伤害。但是，从安全角度来看，有太多的休眠登录可能是非常危险的事。

想想看，如果应用程序背后的开发人员突然变得流氓、或者黑客入侵该服务的数据库，会发生什么？

尤其是，任何追踪者都会采取撒网式搜罗一切关于您的信息，任何蛛丝马迹对他们来说都是非常重要的线索。

如果数字垃圾没有清理干净，不仅会将您的电子邮件地址甚至家庭地址等重要个人信息暴露出来，并且，还可能会让恶意攻击者进入更大、更重要、更敏感的帐户。

这可能是因为您使用了一项主要服务来登录较小的服务（比如用谷歌/FB账户登陆一个小游戏网页等等类似的情况），或者因为您在不同的帐户之间共享了用户名和密码 —— 这是您最不应该做的事。

您闲逛后就不再使用的帐户越多，追踪者和攻击者就越有目标。

因此，建议的做法是大清洗：整理您留下的数字路径，并关闭所有您不经常使用的帐户，尤其是那些与真实身份想关联的账户。

不幸的是，并没有一个大按钮可以让您一次性做到这一切，但是，通过一些简单的侦探工作和几分钟的业余时间，你就可以有效地擦除这些踪迹。

[image]

返回相关主题：[image]在雷达下低飞：变得难以被追踪的简单方法 S03E07

下面将介绍完成这项防御工作所需要的步骤。

[image]

1、找到它们

首先，选择您实际记住的帐户和应用程序，那些仍然存在于手机屏幕上的帐户和应用程序，或者定期在收件箱中提醒您的东西，因为它们最想念您。

如果实在想不起来了，去电子邮件中搜索一下也是好主意 —— 所有用过一段时间的邮箱，尤其是陈年的邮件，很可能会提醒您关于一些曾经的注册行为。

想想您在开设账户时收到的电子邮件中最常见的字眼是什么？—— 搜索“确认您的电子邮件”、或“新帐户”、或“验证您的电子邮件地址”，等这些短语，应该会能找到东西（别忘了使用双语：”confirm your email” or “new account” or “verify your email address”，或者您使用的其他语种）。

您可能正处于甚至不记得手机上某些应用程序是做什么的阶段，因此，浏览您安装的所有应用程序，以识别您不再使用的东西。

[image]

返回 - 工具：[image]彻底卸载

继续，前往您的 Facebook、Twitter 和 Google 帐户（那些您最常用的寡头服务），查看您已连接到他们的所有应用程序和服务，例如，所有“使用 Facebook 登录”按钮。

点击此处查看 **Facebook**，此处查看 **Twitter**，此处查看 **Google**。如果您尚未登录，则需要登录。

从 Facebook、Twitter 和 Google 断开第三方应用和服务通常只需要从上面那三个页面上点击一两下，但是请记住，这实际上不会关闭您未使用的帐户 —— 这只是意味着他们无法轻易进入您的主要帐户了。

最后同样重要的是，查看用于管理密码和登录的任何程序，无论是专用密码管理器还是Web浏览器。

这里面应该会出现一些您已经忘记的帐户，并且还有一个额外的好处，就是，在您忘记这些帐户的情况下这些应用可以向您提供登录详细信息。

[image]

返回：[image]什么是凭据填充攻击？如何选择密码管理器？

2、关闭它们

现在就可以开始实际关闭这些帐户了，如果可能的话，建议最好通过桌面**Web**浏览器完成。

仅仅从手机中移除应用程序是不够的，尽管您也应该这样做。

如果您忘记了特定网站和服务的登录凭据，则必须完成帐户提供的任何密码重置选项，否则您可能需要直接联系客户支持。这很麻烦，但为了安心，这是值得的。

一旦进入这些帐户，就可以寻找任何类型的数据备份或导出选项，不论您想要保留在此僵尸帐户中积累的数据还是将其移动到其他位置。

某些服务会自动查找和删除旧帐户，通常是为您搜索收件箱或社交媒体帐户。

不过我们并不是特别推荐这些服务；因为您无法确定这些服务对您的数据做了什么，而且您必须注册另一个数字帐户才能使用它们。

坚持自己动手是最靠谱的。

现在终于准备关闭僵尸帐户了。

如何处理这个问题会因应用和服务而异，但您应该可以通过快速搜索轻松找到该选项。

您通常需要再次输入密码才能证明您就是您所说的人。

如果您完全找不到方向，JustDeleteMe 有一个方便的数据库，用于删除许多流行服务的帐户。

仔细阅读屏幕上显示的任何信息，特别是有关数据保留的政策：在公司完全清除其记录之前，您可能需要采取一些额外步骤，例如勾选其他方框或发送后续电子邮件。

等待收到确认消息，您就完成了。

[image]

3、注意的问题

1、电邮

在清理的过程中，要考虑的最重要的帐户就是您的电子邮件 —— 所有邮箱，即：您在线生活的中央数据中心。

您的电子邮件帐户对于攻击者来说将是一个宝贵的大礼包，因为它可能包含除了您自己之外的许多其他人（朋友、家庭成员、同事、等等）的信息。

删除您不再需要的电子邮件、并将您仍希望使用的旧电子邮件导出到硬盘驱动器，是一种明智的方法，可以减少因电子邮件被攻击而受到损害的可能性。

几乎所有电子邮件服务都提供导出邮件和其他帐户数据的方法，以便您在本地保存，并可以从公司的服务器中删除它。

并且，不要忘记清除和删除不再使用的旧电子邮件帐户。

如上所述，您还应该利用电子邮件搜索功能来梳理旧邮件。

您可以批量删除特定日期之前的所有内容、或特定联系人相关的所有内容。例如，搜索旧房东或雇主的名字、删除您发送过的任何电子邮件，因为这些电子邮件中更有可能包含税务表格或工资单等个人信息。

您还应该定期在电子邮件中搜索您的社会安全号码/银行卡号码/身份证号码/真实手机号的最后四位数字，并删除曾经显示过这些号码的任何邮件。

如果可以，请询问这些电子邮件的发件人或收件人，要求对方也将其删除。

[image]

今后请秉持零收件箱原则，干净整洁最安全：[image]最低程度的技术性获得最大幅度的安全提升：如何在敌对环境中保护自己S02E02

2、云服务

和拇指驱动器一样，您还可能曾经在各种服务中随机保存文件，这些服务提供如 Box、Google Drive 和 Dropbox 等免费存储空间。

请对那里的内容进行整理，并消除可能造成特定风险的任何东西 ——例如旧的纳税申报表或财务文件、拍摄了您和重要联系人的照片、视频、等等，描述了您的真实信息一切文档。

[image]

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

3、数据碎屑

您的照片是否备份到了多种不同的服务上？清理一下；您是否还拥有两年前使用过的消息应用程序帐户？为什么2014年的卡路里计算应用程序仍在您的手机上？…… 取消并删除一切。这些类型的暴露都是不必要的风险。

再一次提醒，不要只是从手机中删除应用程序，请确保清理并关闭您的帐户，以便它保留尽可能少的关于您的数据。

4、查看服务条款中的数据处理政策

关闭帐户并不一定意味着公司会删除您的所有数据或删除它所了解的基本信息 —— 数据处理流程应该在应用程序的服务条款中列出 —— 它们有可能会使帐户保持活跃并可能继续收集数据。

5、移动设备相册

智能手机的相册上是否有信用卡、身份证和驾驶执照的照片？朋友和家人在旅行和绑定时是否曾录入过您的身份信息？您是否曾经因某种申请而扫描了您的家庭成员的护照和其他文件？……

回忆所有这些细节。

[image]

高风险用户建议从“威胁知识库”进入该主题 - “分身”。

6、讲卫生最安全

全部清理完成后就可以以全新的身份开始新生活了。请尽量记住这些最佳实践，因为您不可避免地会积累积累更多的数字残骸。应定期执

行清理。

任何一次下载和免费使用之前请三思。

好了就是这样。

不论您是否准备人间蒸发，本系列提供的知识都是很有价值的 —— 只要您不喜欢被追踪监视。

[image]
[image]

如何欺骗，和如何防骗：反侦基础课 S06E07

[image] 关键词	审讯心理学 社交工程 社交工程攻击
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月17日
[image] **Description**	行动安全性；心理安全

在现实中您能遇到的伤害、攻击和威胁，几乎不存在 “正面刚” 的形式，它们中大多数都是从欺骗开始的。 也就是说，如果您能准确识别欺骗，就能及时躲避大多数威胁。

- Table of Contents

  认知偏差
  1、 情感启发
  2、 诱导效应
  3、 鸵鸟效应
  4、 乐观偏见
  5、 近因偏差
  不要因为认知偏差而上当受骗
  骗子如何利用您的心理弱点
  1、 互惠法则：当您不愿回报人情
  2、 为什么不能总是乐善好施
  圈套
  如何识别圈套
  分心术
  如何操纵目标人按照您的意图行事
  社交工程如何为您所用

1、雇个保镖
2、借个孩子
3、假装应该到场的样子
4、投其所好
如何撒谎和如何识别谎言
建立基准线
策略1：让他感觉舒适
策略2：询问他明显知道答案的问题
策略3：仔细观察
撒谎时的行为
1、开始的3～5秒
2、不直接回答
3、脚
4、僵硬
5、过度盯视
6、过度反应
7、不直接回答
8、头部动作
如何欺骗测谎仪
1、识别您被问到的问题类型。
2、必须隐瞒自己对测谎的了解。
3、了解测试者在寻找什么。
4、 提前练习对策。
5、要把整个测谎日当作一次完整的考试来对待。

[image]

本站关于社交工程的主题内容汇总在 🍎 心理安全-PsychologicalSecurity 中。

社交工程其实不是个坏东西，它只是种技巧，而且是运用非常广泛的技巧，虽然它总是被与欺骗联系在一起。中文流行语“拿捏”，就是一种常见的社交工程。

社交工程的确是一种心理操纵，它通过入侵人的心理弱点和情感bug，达到控制行为的目的，让目标做出原本不想做的事。它可以偷走您的银行存款，也有可能帮您戒烟，既可以让焦躁的朋友冷静下来，也可以骗取您的密码以入侵您的账户 …… 这取决于使用目的。

对本站的主题来说，我们只关注恶意的使用，即纯粹的欺骗和防骗的方法。

欺骗是一门艺术，骗子高手都很擅长玩弄人性弱点，对其加以利用从而达到他们自己的目的。他们是情感游戏大师，深谙各种人类情感 —— 贪婪、好奇、慷慨、恐惧 —— 的操控方法。

类似恐惧这种情感能够帮助您摆脱麻烦，比如在被追杀的时候刺激您的行动力以帮助逃命、在发生火灾的时候警告您的快速反应；但是，这些情感也能把你困住，骗子只要能激发您的刺激性情感，就能控制您的行为。

准确说，上当受骗的人并不是输给了社交工程师，而是输给了自己的认知偏差。

延伸：https://web.archive.org/web/20201027152545/https://www.iyouport.org/%E4%BA%BA%E4%BB%AC%E4%B8%BA%E4%BB%80%E4%B9%88%E7%9B%B8%E4%BF%A1%E9%AA%97%E5%AD%90%EF%BC%9F/

延伸：https://web.archive.org/web/20191121120235/https://www.iyouport.org/%E6%88%91%E6%98%AF%E5%A6%82%E4%BD%95%E4%B8%8A%E5%BD%93%E5%8F%97%E9%AA%97%E7%9A%84%EF%BC%9F/

我们先说说如何防骗，然后再说怎么骗人。

了解如何防骗的最佳方式是：了解欺骗是如何生效的。

认知偏差

即便您平日很擅长思考，也无法完全避免认知偏差。

其实认知偏差并不完全是坏事，它是一个捷径，是一种保护机制。人类需要处理各种各样的信息，有时需要立即做出决定，而认知偏差就是大脑在帮助您更快决策时所采取的捷径。

但是，当遇到骗子的时候，认知偏差就会让您陷入麻烦。不过如果能学会警惕几种关键的认知偏差，就不会被骗局所伤害。

1、情感启发

情感启发就是让您立即做出本能反应。这是一种迅速发生的即时反应，通过情绪促使您做出决策。

一般情况下，如果对某个事物有好感，人们就会倾向于推测它会带来有益的影响。换言，您的主观感觉会为您对特定情境的解读添油加醋。

举例：如果小时候您在和家人一起度假游泳的时候获得了很多快乐，那么水这个意象就会给您带来愉悦和平静的印象。相反，如果童年时期差点溺水死亡，水就会让您感觉不安和恐惧。

对水的感觉会直接影响您在现实中对水这一事物的反应。

2、诱导效应

诱导效应就是在两难抉择之时，让您“意识到”还有第三种选项。“选项3”能让您轻松在前两者中做出选择。

杜克大学的营销专家曾经通过询问一组人的选择偏好，解释了诱导效应的工作原理。

一种情况是，真正超赞的五星级餐厅还要开车走很远，而另一家三星级餐厅就近在咫尺。他给您的选择就是：究竟是为了美食长途跋涉，还是就近就餐，放弃美味？

被测试的这群人无法决定。他们都觉得，如果距离不是那么远的话，五星级餐厅绝对是想都不用想的答案。于是营销专家引出了选项**3**：一家坐落在这两者之间的两星级餐厅，

正是这个选项的出现激发人们选择了就近的三星级餐厅，因为它不论位置还是品质，都胜过了那个选项3。

举例：星巴克有小杯、中杯和大杯，当有了超大杯或高杯的新选择时，多数人都没有考虑附加的选项，也没有选择平时自己会选的小杯，而是直接挑了中杯。

诱导效应就是导致人们下意识地将其他选项与所谓的“新选项”做比较，然后选了稍微大一些的中杯。

3、鸵鸟效应

当听到好消息时，人们就会希望越多越好；如果是坏消息，哪怕是有用的坏消息，人们也一般宁愿不知道。

就如鸵鸟，把头埋在沙子里，“看不见就相当于不存在”。

举例：鸵鸟效应非常普遍。比如对信息战的揭露如此之多，但那些虚假的用来心理操纵的账户始终在那里、尤其是始终看起来如此受欢迎。揭露几乎没起到任何作用，甚至揭露的文章都很少有人关心。

延伸：https://iyouport.substack.com/p/--c32?utm_source=publication-search

再比如，在花了一大笔钱度假或庆祝节日之后，您会不愿意打开信用卡账单。您知道消息会令人不快，所以就扔在那里直到不得不打开。

4、乐观偏见

人们希望保有进步的期待，喜欢保持乐观而非采取现实的态度，希望事情比实际要更好。这是一种积极心态，但是，也意味着对潜在的危险毫无防备，处于弱势。

举例：对未来完全乐观的人可能对实际上很有可能发生的大事缺乏准备。也许没有足够的储蓄应对失业危机，也许不会找医生去做年度体检。一旦发生灾难，这样的人很可能会措手不及。

5、近因偏差

近因偏差指的是，人们倾向于认为近期发生的事 —— 自己当下所看到的任何趋势和模式 —— 可能会影响到未来。人们很容易记住近期事件的影响，因此不喜欢从实际数据出发。不愿承认存在不可测的概率，相反，人们倾向于预估生活会沿着相似的轨迹前进。

经济学上的黑天鹅这个词您一定不陌生。

举例：您可能会认为本地近年来都没有过飓风，就不把飓风警报当回事，拒绝采取适当的防御措施。

不要因为认知偏差而上当受骗

以上只是一些最常见的认知偏差，完整的认知偏差列表比这些要长得多。您可以学习一些方法以避免由于认知偏差而上当受骗。

保持合理的怀疑是保证安全的关键。这并不是说您需要整天担惊受怕，而是说您的态势感知能力必须可以及时提醒您关于危险出现的可能性。

比如在街头，陌生人求您看地图指路的时候，请先花一分钟看看自己身后和周围，有没有奇怪的其他人、有可能埋伏着什么；再比如，当有人敲门自称警察的时候，先拨打当地警局的电话以确认门外的人究竟是不是警察。

保持警惕，不要害怕检查周围环境或验证信息，这样才能保持安全。还记得S03系列中强调的宗旨吗 —— 零信任，始终验证。

[image]

骗子如何利用您的心理弱点

每分钟都有骗局发生。尤其是在互联网时代。没有人能列举出所有骗术，但是本文希望列举一些最常见的骗术，如果您能熟悉它们，就可以在遇到同样状况的时候立即反应过来并加以避免。

1、互惠法则：当您不愿回报人情

我们都遇到过真诚地想要回报善意的情况。如果邻居在您出差时帮您接收保管邮包、在紧要关头同事帮您带过孩子，您一般都会很愿意回报对方的好意。基本上，只要有人付出过善意，我们都会愿意回报人情。

但是，在某些情况下，这种自然而然的回报心理会带来大麻烦。当骗子蓄意利用互惠心理，索取比付出更大的事物作为回报时，您就会陷入危险。

这是社交工程中最常用的手段。它可以从请您喝东西开始，或者送您小礼物，接着就是索取小的回报，而这样看起来不起眼的回报索取往

往就是灾难的开端。甚至有人因此最终替人行凶杀人。

底线是，即便您欠了别人的人情，也不要处于羞愧而做出会让您感觉不妥的事。回报是一回事，作恶就是另一回事了。

2、为什么不能总是乐善好施

一个真实案例。一位女士在加油站遇到一对夫妇，其中妻子问她能不能借点钱加油。这位女士同意帮忙了。那个妻子表达了谢意，说“你真的帮了大忙，你是好人，我能抱抱你吗？”然后很开心地拥抱了她一下。

接着那名丈夫从店里走了出来，也对她表示感谢，并同样说“我能抱抱你吗”。直到第二天早晨，这位女士才明白为什么那两次拥抱不对劲 —— 她的银行账号里的钱全没了。

就在她从加油站离开之后，她的银行卡发生了两次大笔支付，也有从自动提款机提款。事实证明，就在拥抱的时候，那对夫妇扫描了她口袋里的银行卡信息，然后实现了身份盗用。

这名女士还算幸运的，只是被偷了钱；乐善好施是好事，但如果您遇到的是骗子，甚至有可能会付出生命的代价。

您应该保持警惕，试想有可能发生的一切问题，而不是盲目地答应任何事。

70年代臭名昭著的连环杀手“Ted” Bundy 就是这样诱骗受害人的。他在自己手上腿上绑着石膏，伪装成受重伤的样子接近行凶对象，请求对方帮他搬东西。看到一个“伤成这样的人”还需要搬运那么重的东西，人们普遍会答应帮忙 …… 结果就是被他引诱到暗处并被杀害。

当然，绝对不是说每一个寻求帮忙的人都是连环杀手，但这个案例的

确能说明，看似简单的举动也有可能带来非常危险的后果。

不要轻易上陌生人的车，在不确定对方身份的情况下不要给陌生人开门，不要把自己的身份信息包括住址和家庭成员及朋友的信息公开给陌生人 —— 包括在互联网上，这是最基本应该做到的。

圈套

设套就是指编造一个情境引诱人上钩，让对方做出平常状态下不愿做的事，或泄漏一般情况下不愿泄漏的信息。比如网络钓鱼，使用的就是这种方法。

设套需要一个精心制作的谎言，骗子会冒充您的同事、银行雇员、保险调查员、税务人员、警察、甚至牧师。只要假冒身份可以拥有将目标人置于某种特殊情境的权力，或者有权让您说出特定信息。

如何识别圈套

设套的人一般都已经预先准备好了答案，他希望获知需要了解的信息，以便给人以权威感。

成功的设套者反应机敏，不论情势如何变化，他都能做到从容应对。相信您的直觉，要明白如果此人不能回答所有问题，事情就不对劲。举例来说，如果有一个家伙示意您靠边停车，但他既没有穿制服、他的车也没有标志。

细节不合理是不难觉察到的。比如一个人告诉您：“我只不过是搞了一个小型家庭聚会”。然而他楼下停了几十辆陌生的车子，整条街都能听到音乐声。

有些圈套会看起来好得让人难以置信。如果有人说他有一笔钱等着给

您，或者您中了什么奖，不要信，基本可以肯定是骗子。

信用卡公司不会打电话来询问您的私人信息；如果开卡公司打来电话，那就直接挂断，然后拨打卡片背后的电话号码询问那是为什么。

[image]

分心术

从本系列第一集开始我们就强调了对分心术的警惕，因为这是一种非常常见的攻击方法。还记得美女和大卡车的比喻吗？

人们很容易分心，而攻击者深谙此道。他们会选择一个人或一群人，设计一套分散注意力的方案，这并不难，并且屡试不爽。

曾经在一个小镇里，有人打电话给警察局谎称学校附近有炸弹，警察很快找到了打电话的人。而当警察忙着调查所谓的炸弹时，一群人把银行抢了。

当然，大多数分心术的使用都非常普通，比如一个美女走过来借火点烟，而您转身就发现自己的钱包没了。

分心诈骗和其他所有诈骗形式一样，具有超级的想象力和创造力；恶意者会使用什么样的方式分散你的注意力？答案可以数不胜数，那么该怎样防御呢？

- 保持距离。如果事情看起来不对劲，先退后，不要让那人接近您，这样至少能先阻止对方盗窃或袭击您；

- 注意身后。如果有陌生人靠近您，不论是小孩还是老妇人，不论是问路还是想搭便车，您需要立刻注意的是自己的盲区 —— 身后的四周 —— 小心在您的盲区里潜藏的埋伏。

- 提问。多问问该人的经历，确认一切是否合情合理。不要听信对方的表面言辞。如果他想要分散你的注意力，是不可能答出您提出的所有问题的，您一开始提问，他们就会逃跑。

[image]

返回 - 自卫措施：[image]背景调查 ；[image]关系网络图谱

以上是最基本的防骗方法。了解它们能帮助您抵御大部分以欺骗为踏板的攻击手段。

下面将介绍的是，如何骗人。

如何操纵目标人按照您的意图行事

不论是在社交媒体上（尤其是私密群组里）、还是在酒吧那种小空间里，总是容易遇到有人跑来和您主动分享他们自己的秘密。请注意，您无法确定您听到的对方的“秘密”究竟是不是真的，然而在这种环境下 —— 看起来就像是被信任的交流中 —— 您很容易被诱使着顺口说出自己的秘密。而您说出的东西很可能是真实的。

在当下这个人际疏远的时代里，一旦有人愿意吐露真心，很多长期忍受孤独的其他人都会容易被激励着用自己的故事去回报。不要这样做。在您听到对方似乎敞开心扉的时候，要保持警惕，随时记得，一旦您说出了任何信息，它们都将脱离您的控制，任由对方使用。

喝酒之后尤其要注意这点。最好是能保证自己不要在有不十分信任的人在场的环境中饮酒。

社交工程如何为您所用

当然，首先，您不应该去伤害别人。只是，您也许可以用它来找点乐

子，在反抗行动中也是可以采用的 —— 把警察和当局绕进死胡同。这需要漂亮的创造力。

下面将总结几个最容易起效的社交工程手段，您将能从中发现应该注意哪些问题才能做到有效防骗。

1、雇个保镖

您有没好奇过，当名人是什么感觉？

纽约州立大学的学生 Brett Kern 就用社交工程手法找到了答案。

[image]

Kern 首先查看了纽约时代广场的地形，觉得那里是作为名人首秀的完美舞台。于是他给自己找了2个随从，从网上雇了2名保镖、3名摄影记者、4名摄影师。

相貌相对普通的 Kern 换上了帅气的衬衫、戴上深色墨镜，外加一脸灿烂的笑容。

他小心翼翼地走出洛克菲勒中心30Rock大楼，两名看起来高大严肃的保镖走在他的两侧；摄影记者和摄影师准备好开工。

Kern 露出灿烂的笑容，表现得很自信的样子，他对人群连连飞吻。人们立刻接受了这一套。

Kern 的朋友在人群中随机问人们对 “著名的 Brett Kern 有什么看法”。其中一名男士表示 “他是很棒的演员”，甚至还提到《蜘蛛侠》中明显不是 Kern 扮演的角色。而另一个人被问到 “对 Kern 的音乐有什么看法”，对方立刻回答 “曾听过他的首支单曲” ……

粉丝们追随 Kern 在时代广场逗留了近3个小时，他也频频摆出姿势和大家合影。一群尖叫飞吻的小女孩高声喊着 “这是我人生中最幸福的

一天！我爱他！他好帅！”

闹剧进行到最后，Kern 身边还有好几百人。考虑到大规模聚众容易引来警察，Kern 在保镖的护送下进入了一家小酒店，然后独自一人坐地铁离开了那里。

这是个很完美的社交工程 —— **Kern** 通过构建一个大众熟悉的场景，甚至诱骗人们产生了幻觉，感觉自己似乎 “认识这位明星”。

这种效应其实并不奇怪。您经常能在互联网上看到大量的标题党文章，如果阅读这样的文章过多，人们就倾向于认为 “互联网上都是这样的文章” —— 某种情境就确立了。人们会下意识地给任何来自互联网的文章贴上这样的标签，从而埋没了那些认真写作的人。

2、借个孩子

如果您想让目标人卸下防备，借个孩子可能会很管用。

老实说，这种手法也许只对男性有用。显然，大多数人都像是被洗了脑似的，会毫不犹豫地信任一些被社会视为 “理所当然” 的东西，比如，男人不擅长带孩子、年轻人总是很冲动、老人都是愚蠢的 …… 等等，您知道，这其中显然会有非常多的特例，以至于这些观点几乎都无法成立。

而骗子，最擅长利用的就是大众的这类认知。

如果是一名女性带着婴儿，没有人会多想什么。但如果是男人带着婴儿走出杂货店，提着大包小包的东西？也许他会被评为 “年度最佳父亲”？

如果一名男性带着一个哭闹的婴儿在公共场所寻求帮助，大多数人都会被启动恻隐之心，人们会认为这个男人几乎走投无路了。

很傻是吧？现实中这种傻事其实比比皆是。

3、假装应该到场的样子

在电影《Wedding Crashers》中，Jeremy 和搭档 John 最擅长闯入各种婚礼，哪怕是年度最受瞩目的 —— 财政部长家的千金的婚礼。

他们大摇大摆地走进去，自我介绍一番，喝着香槟，毫不犹豫地捏造出各种受邀的原因。

假装应该到场的样子，这种方法很有效，能帮您闯入各种本不应该出现的场合。不要做不速之客，不要做坏事，不过看看人们如何绞尽脑汁还是很有趣的。社交工程师可以泰然自若地假装成任何业内人士，进入他们本无权进入的地区。

[image]

当被要求检查身份卡时，粗制滥造的假货也能蒙混过关 —— 气质和神色经常比身份证明更管用。

如果 Jeremy 和搭档 John 鬼鬼祟祟、衣衫褴褛出现在财政部长家千金的婚礼上，肯定会立刻被赶出去的。进入您原本不该进入的场合意味着，您需要表现出对周围环境了如指掌的样子。

这需要您真的了如指掌，也就是需要事先做好充分的调查，您需要知道哪里有什么，不要到了那里才东张西望。行为必须自然潇洒，才能看起来像 “自己人”。

4、投其所好

这似乎无需过多解释。骗子在这方面有天生的嗅觉。

在任何一种安全防御中我们都会强调，切勿让陌生人对您了解太多。

这点真的非常重要。了解您的人就可以利用您和操纵您。

每个骗子和攻击者都知道调查的重要性。开源情报是任何一种行动的基础工作 —— 您对目标的了解越多，就越能设计出最有效的渗透和攻击策略。

[image]

作为防御者，您的基本目标就应该是，尽可能少地暴露自己的私密信息，任何私密信息，包括那些看似无害的信息只要与您的私生活相关。因为您肯定不知道这些信息一旦被恶意者掌握，会被如何使用。

社交媒体很危险在于，它倾向于促进人们表达自己的内心，它给那些喜欢 “晒生活” 的人以更多的关注度 “鉴赏”。不知不觉中，人们就会说出一些很致命的信息。

就算是喜欢的乐队、钟爱的电影、曾经做过哪类工作等等信息，都完全可以被用作社交工程手段，从共鸣点获取你的信任，从而深入操纵你。

他人对您的了解越少，您就越安全。任何时候都是如此。当然，我们都会为了某种需求与某类人交换一些个人信息，比如你必须告诉医生关于病史和过敏情况，再比如你必须告诉人力资源招聘者关于您的学历和能力、甚至性格特征，但必须到此为止，请衡量对方对您的价值 —— 关于他们能提供什么，将信息暴露仅限于满足获取其价值的程度内。越少越好。

[image]

返回：[image]结识新认识的人时您应该曝光自己多少信息？- 原则和技巧

返回：

如何撒谎和如何识别谎言

每个人都会撒谎。包括还没学会说话的婴儿都会用假哭来骗取妈妈的更多关爱。但是这里希望解释的“会”撒谎是指，难以被识破的那种谎言。

这不是所有人都能做到的。大多数谎言很容易被识破，嘴巴在说谎，但身体却拼命想要保持诚实。而撒谎高手是足以避免这点的。

大多数人在撒谎时都会表露出一些特征，其实不同的人之间这些特征并不完全相同，于是当您看到某种“总结”式的识别谎言教程时，您应该知道，那本身可能就是撒谎。

识别谎言有很大的经验成分，想要用文字总结它们可能并不那么容易；但的确有一些规律/流程可以遵循。

首先第一步就是，构建基准线。没错，就如前文中对识别危险的介绍中指出的技巧。

一名父母也许很容易看出自己的孩子是否撒谎，一起生活多年的夫妻之间也很容易察觉到对方欲言又止的样子；但是大多数危险的欺骗都来自陌生人，那些您完全不了解的人。要识别陌生人的谎言最重要的一步就是，在尽可能短的时间内将对方变成“熟人”。

想想看，您为什么会能立刻觉察到女朋友撒谎？那是因为您了解她不撒谎时的样子，并看出了某种不同的出现。了解 —— 这就是基准线。

[image]

对于一个需要被考察的陌生人，您可以先问对方一些他基本不可能也没必要撒谎的问题，并仔细捕捉对方的特征 —— 在不撒谎情况下的特征 —— 快速记住它，作为此目标人的基准线。在接下来的交流过程中，如果任何一个时候您发现对方出现了偏离这一基准线的表现，

再次记住它，并记住这是在哪个话题下发生的，那个话题上对方有可能在撒谎。

这是审讯中警察最常用的方法。对于一名嫌疑人，警察会先提问 “你叫什么名字”、“住在哪里”，事实上警察手边的档案夹里面都有此人的详细信息，理论上完全不需要再问一遍，但为什么要重复这个过程呢？正是因为他们需要通过这类简单的问题来抓住嫌疑人的基准线，以便在接下来的重要提问中判断对方是否撒谎。

擅长识别谎言的好处太多了。我们每个人都需要不断与他人交流，需要判断生意合作伙伴、雇员、邻居、熟人和那些和试图和我们的孩子打交道的人是否足够可信，如果误判，后果可能会很严重。

相反，如果您准备骗人，请尤其注意这些细节 —— 反用这些方法，努力避免在此出现破绽。

[image]

返回：

建立基准线

如上所述，您首先需要快速了解到目标人在正常状况下的表现，也就是不撒谎的时候是什么样子。那就是基准线。如果不能准确地抓住基准线，您很可能在对方撒谎的时候也难以觉察出来。

那么如何掌握基准线呢？

有几种策略。这还是要引用审讯场景，或者被政府间谍问话的时候那种场景。您经历过被国安局喝茶吗？回想一下当时那些间谍的对话模式？是的，他们非常模式化。

策略1：让他感觉舒适

也许您总是从电视剧和电影中看到酷刑式的审讯场面，警察通过折磨犯人来逼迫其认罪。但这只是一方面，在现实中，通常情况下的最佳做法是，确保您想要建立基准线的对象处于舒适的状态。

[image]

让他在沙发上坐下来，给他倒杯水，空调开到最佳效果……这样的方式才能确保您得到准确的基准线。尤其是在以套话为目标的审讯中，警察和间谍都会采用这种方法。

如果在30多度的太阳底下、双方都大汗淋漓的状态下，您无法判断对方是否撒谎；如果您非常了解对方，很清楚他害怕的是什么，也无需去判断。如果对方恐高，那么您就不能在帝国大厦的楼顶判断他是否撒谎；如果您知道对方怕狗，您就不应该在对话时把狗拴在身边。

策略2：询问他明显知道答案的问题

在尝试建立基准行为时，您应该问对方一些他明显已经知道答案的问题 —— 他完全没有理由撒谎的问题。

比如，如果您知道对方曾经在阿里巴巴工作过，那么就可以这样问他“你在阿里巴巴工作过吗？那里的环境怎么样？福利好吗？”因为这种简单的问题对方完全没必要撒谎，于是他的回复就能帮您找到一些准确的线索，以了解此人在说真话的时候是什么状态。

策略3：仔细观察

在对方回复这些完全无害的问题时，您需要仔细观察，由此来发现他尽可能多的习惯或行为特征。

[image]

快速记住他在回答问题时做过的所有事 —— 每一个微小的行为细节，以此作为基准线。

比如抖腿的节奏、玩头发、咬指甲、不同寻常的面部抽搐和表情、眼睛向下看、叹气、清嗓子、玩衣服（整理领带、衣领、袖子等等）……

如果您能够注意到人们在说真话时的特殊行为，那么当他们撒谎时，您就很容易觉察到了。

撒谎时的行为

请注意，如上所述，撒谎的人不会表现出您在所有同类教科书中读到的完整特征。并且，如果某人表现出了其中某一项特征，也不能就此认为他在撒谎。

[image]

您需要寻找的是一组行为特征：此人是否表现出多项信号行为？这一组行为明显偏离此人的基准线，那么他可能就是在撒谎。

1、开始的**3～5**秒

如果某人在撒谎，在被问到与谎言相关的问题时的前3～5秒内，他可能会表现出一些信号行为。也许会出现结巴、或无法表述清楚。在回答问题时他可能在一些细节上磕磕巴巴。这是因为大脑在编造谎言的时候需要时间。

3～5秒是个一般性的窗口期，如果是接受过训练的撒谎者，这个时间会更短，几乎难以被捕捉到。所以要特别仔细地观察。

2、不直接回答

内疚的人不会直接回答您的问题。

内疚的人会首先列举您应该相信他们的原因。他可能会开始讲述自己的优点，或者您会听到他提起曾经如何帮助过您（暗示您应该感恩），等等。

虽然他可能确实帮过您，但这不能做为替代真相的理由。

诚实的人会直接回答您的问题，而不是想方设法证明他自己为什么“应该被信任”。

3、脚

曾经有人多教科书告诉您如何通过面部表情来识别谎言，他们称之为“微表情”，也就是那些一闪而过的细节，比如嘴角、眼睛等等。其实并不尽然。

在识别谎言方面，双脚的动作也许比面部表情更容易泄漏撒谎的信号。

如果和对方坐在桌边或沙发上，当你问起一个潜在的威胁性问题时，他的双脚开始抖动，而此前则没有这样，那么有可能他在撒谎。

在其他情况下双脚也会泄漏信息。仔细观察，双脚会自然而然地指向他们需要前往的方向。

举例来说，当您在派对上和某人交谈的时候，如果他的脚指向门外，那么从某种程度上说，他可能是想要离开（对您的兴趣不高）。

间谍机构和安检人员的训练课程中就包括这点：观察人们的脚。诚实的人在交流中他们的脚很可能会指向您—即对话者，而不是其他任何地方。

双脚比脸暴露的信息更多。

4、僵硬

僵硬就像是一种缩进乌龟壳中的动作。最常见的情况是，心怀愧疚的人会减少活动，身体僵硬。

也许这种僵硬不那么突出，还是那句话，您需要仔细观察，与基准线做出明确的对比。

5、过度盯视

眼睛当然可以为一个人是否撒谎提供线索，但并非是绝对必要证据。

许多人认为一个人撒谎的时候会眼睛下坠，但也有非常多的情况下多数人的眼睛会向上看，也或者干脆是死死盯着你。

对方是在借助直接的目光接触来证明他自己的清白 —— 努力地想要说服你 “这是事实”，但这种盯视并非普通人的正常行为。

6、过度反应

撒谎的人与人对峙时很容易出现过度反应。他们的目的是击败您 —— 让您的质疑显得荒谬。

想知道女朋友有没有外遇？可以采用这种方法，与她对峙。如果她表现得很惊讶且似乎相对淡定，那可能说明您的怀疑是错误的。但如果她大发雷霆，为您的“不信任”深表痛心，请注意，这可能是危险信号，说明您的外遇推测一定程度上准确。

换位思考，如果对方说错了，您会当它是个玩笑，而不至于大发雷霆对吗？只有在对方把您的阴暗面猜对了的时候，才会最具刺激性。

7、不直接回答

如上所述，忽然转向自辨而非回答问题，这是一种撒谎的迹象。还有一种回避方式就是，对方会通过反问来回复您，或者根本就拒绝回答。这些都是有可能存在撒谎的暗示。

8、头部动作

摇头可能也是撒谎的迹象，但这是最不容易察觉的一种。如果您问某人问题，而他的回答是真话，那么他的头部不会有可见的奇怪动作。

反之，如果对方在开始回答问题的时候微微点头或摇头，那么他可能是在撒谎，或者不够真心。

仔细看，您会能注意到对方说出的话和头部动作不一致，也就是他的头部动作没有在解释或加强他自己说出的话，有些时候是语言和动作完全相反，这就很可能表明对方没有说实话。

[image]

返回：

如何欺骗测谎仪

也许您已经读过一些关于如何欺骗测谎仪的读物，说实话，和上面的肉眼测谎一样，那些出版物中介绍的东西不一定都是真的。

测谎仪是个非常不可靠的东西，事实上它不是在 “测谎”，而是在检查您的血压心跳脉搏等生理指标的稳定程度。它建立在一个完全不现实的判断上，即 “撒谎的人会出现这些生理指示的变化”。

为什么说它完全不现实呢？因为可以通过训练来避免被捕捉到生理变化。也就是欺骗测谎仪的办法。

欺骗测谎仪的关键在于：您不要害怕它。这可能说起来简单，但实际上被那堆电线绑住身体后，大多数人都会有一些紧张。千万不要，如果你的心不够稳定，就很容易被捕捉到谎言。

[image]

您必须保持平静，让自己深信自己说出的每一句话。你越是冷静，它就越对你没办法。

大多数情况下您可能不会遇到测谎仪，但万一遇到。您必须知道一些事，以保证您的安全 —— 正因为这个东西不靠谱，所以它有可能将您的紧张心态视为 “谎言” ，进而耽误您的伟大事业，甚至让您陷入麻烦。

要想骗过测谎仪，首先需要记住下面**5**点注意事项。

1、识别您被问到的问题类型。

您会被问到的问题基本有三种类型：相关问题、无关问题和控制性问题。

无关的问题是那些显而易见的问题，也就是说您无需撒谎的问题（如上所述，和肉眼测谎的基准线一致）比如 “你叫什么名字？” 或 “这个房间的灯亮了吗？”

相关的问题是那些重要的问题，比如 “你是不是把那份备忘录泄露给了媒体”、“你是否黑入了雇主的账户？” 或者 “你有没有卖过毒品？”

控制性问题是指那些你对相关问题的反应作为基准线将与之进行比较而设立的问题。这些问题通常是（几乎）每个人都能回答 “是”、但每个人都不愿意诚实回答的问题。例如，”你是否曾经为了摆脱麻烦而

撒谎？”或 “你是否曾经从雇主那里拿过任何有价值的东西？”

2、必须隐瞒自己对测谎的了解。

测谎师可能会在测试前问您，您是否对测谎测试做过任何研究，或者您对测谎测试有什么了解。千万不要透露您做过广泛的研究。需要表现得好像您对测谎一无所知，但确实相信测谎是一门科学，测谎仪是可靠的（或至少不要表现出对其可靠性的任何怀疑）。

测谎师可能会试图通过提及某些技术术语和缩写词来欺骗您，例如：”你的测试结果是NDI”。虽然您会知道 “NDI “的意思是 “没有欺骗迹象”，但您需要表现得好像不知道它的意思究竟是什么。

如果让他们知道您对这个过程了解太多，可能会让测谎师认为您有什么隐瞒的，即使您没有隐瞒。

3、了解测试者在寻找什么。

测谎仪是为了帮助找出具体的信息，比如是否是间谍、或是否吸毒。

您基本可以肯定能知道为什么被拉到这里来测谎，也就是说您一开始就能知道测谎者在注重考察什么。不论是就业前的筛选测试、研究公司或机构的政策等等，您需要首先明确这些，以确定能承认什么，不能承认什么。

4、 提前练习对策。

事先练习这些，可以大大增加您 “通过“测谎仪考试的可能性，但前提是要做对这些措施。

一定要在考试前好好练习，这样就能彻底做好准备了。

5、要把整个测谎日当作一次完整的考试来对待。

也就是说，并不是直到您身上被绑上电线后 “测试” 才开始 —— 在您通往测试地点的途中、以及您离开此地的过程中，都在测试者的眼皮底下。每一个细微的举止都会被纳入测试结果。

甚至在等候室和洗手间里，也可能有隐藏的摄像头。切记这点，这是非常普遍的做法。

如果您能记住上述这些，那么欺骗测谎仪并没那么难。只需要一个关键，即：您需要深信自己说出的每一句话。不论您说的是真话还是假话，努力从心底去信任自己。您就成功了。

测谎仪捕捉的是您的愧疚和忐忑不安。如果您 “心安理得” 地撒谎，它就无法识别出来。

听起来很难是吧？如果做过某些会让自己后悔和害怕的事，很难做到心安理得，的确；但是，只需要一点练习。

真正危险的是上述 “控制性问题” —— 就是那些通常措辞含糊的或大多数人在此都会有违规行为的问题。您需要快速准确地识别这样的问题，它们就埋在整个测试过程中，不定时出现。

遇到这样的问题时您可以试试下面这些方法：

- 呼气后，等待4～5秒钟，然后再次呼气（或者，慢呼吸几秒钟）
- 在脑子里使劲想那些非常令人兴奋的、沮丧的、恐惧的或令您生气的事
- 咬自己的舌头，足以感到疼痛

也许曾经有些教科书会告诉您“提肛”，就是努力缩紧肛门的方法，但是如今这个方法也许不管用了，因为很多测谎现场都配有超灵敏的坐垫，它会识别您的小动作。

同样，还有一些建议会告诉您“在鞋上放一些钉子”，当上述类问题出现时，去踩钉子，让自己感觉疼痛。但是如果测谎现场要求您脱下鞋子……就麻烦了。

所以，不要尝试那些容易被抓到的方法。当然，希望您不要遇到测谎仪，那东西真的特别讨厌。

好啦就是这样！希望本集的内容能帮助您避免受骗和受害，而不是帮您欺骗善良的人。不要做坏事，这是我们提供的所有内容的宗旨。

[image]
[image]

S08精神心理安全-总章节：唤回心灵

[image] 关键词	互助 变革 心理健康 无政府主义 疗愈 自主
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2025年4月1日
[image] **Description**	心理安全

[image]

这个社会让如此多人处于极其不快乐的境地，然后再卖药给他们以“消除他们的不快乐”。

这可不是科幻小说。现代社会没有消除导致人们抑郁的条件，而是在抗抑郁药市场上赚得盆满钵满。

抗抑郁药物本质上是一种 修改个体内部状态 的手段，使其能够容忍正常人类原本肯定会觉得无法忍受的社会条件。

[image]

S08系列基于以下两个长期立场：

□

返回：

延伸：https://iyouport.substack.com/p/00e?

utm_source=publication-search

[image]

摆脱受害者心态，重塑自我

我们已经被孤立太久了！在经历了这么多年的隔离和异化之后，有些人已经放弃了被真正理解的渴望（是理解，而不是像精神心理医生那样仅仅‘富有同情心’）。

我们应该收回自己的心智。我们不需要各路“专业人士”来告诉我们“应该”如何生活。

> 要么你自己思考 —— 否则就必须让别人为你思考，从你手中夺走权力，扭曲和管教你的天性，驯化和阉割你。 — 弗朗西斯·斯科特·菲茨杰拉德

受害者心态使人们感到必须有某种专业人士的帮助 —— 心理健康工作者、宗教领袖、教育家、时尚顾问，等等所有这些 —— 因为“受害者”无法独立做出自己的决定或开展自己的活动。我们不是受害者。我们都有能力找到自我疗愈的方法，正是自我怀疑和无力感让我们停滞不前的！

谁能比你自己更了解你脑中发生了什么？内心深处的恐惧、动机、欲望通常超越言语，它们的触及如此深层，以至于很少有精神病医生能发现它们，尤其是在保险公司的效率算计压力之下。

我们思考和看待世界的方式完全取决于我们过去的经历。没有人能够在不重新体验我们整个生命的情况下真正理解我们。

我们的目的不一定是要全盘拒绝精神病学，而是要让人们选择他们认为对自己最好的方式，向他们展示可用的不同替代方案，并教育他们了解精神健康“行业/商业”的谎言。

最重要的是，我们并不是在寻找一个唯一的“真理”。我们希望每个人都能理解自己的心智是如何运作的，寻找自己的解决方案，并拥有采取自认为最适合的任何行动的自由。

自我探索使我们任何人都能从无助的受害者状态进化为疗愈者。

[image]

传统“疗法”的替代方案是存在的，而且大多数早在专业精神病医生阶层出现之前就已存在了。例子包括：冥想、瑜伽、自我催眠、营养疗法、认知疗法、神经语言程序学（NLP）。所有这些都是我们工具箱中有用的工具。它们中的大多数还具有整体观，强调整体的重要性以及各个部分之间的相互依存性，而这是大多数精神科医生完全拒绝的想法。

[image]

解决方案不会来自上方或外部，而是来自下方和内部。如果你愿意倾听，你的潜意识就愿意帮助你的意识心智进行疗愈。

当我们最终对我们是谁、对我们的生活、对我们的社区、对我们的星球、对我们的未来，承担起责任时，改变就会不可避免地发生。

我们不再被社会的双重言论所愚弄 —— 它一方面告诉我们要成为“负责任的公民”，另一方面又要求我们无条件服从上级的命令。

我们想要真正的责任和真正的自由！

超越疗愈

在这一点上应该澄清一件事：这不仅仅是关于疗愈的。因为疗愈概念暗示存在可达的巅峰、可寻的永恒安宁。除童话和广告外，世间不存在此类境界。请谨记：永久幸福是支配者创造的神话。个人成长（或任何近义词）实为持续循环的过程，其中旅程远比终点更重要。

要想更自由地前行，你就需要卸下所有精神枷锁，尤其要抛弃“自己有缺陷”的念头。更该常记于心的是：你本具自足！你已在现有境遇中竭尽全力，即便至今走过的路比他人更艰难，也绝不意味着你是个失败者！所谓的“正常人”终将经历这番洗礼，否则他们永远无法真正成长。

你相信自己是什么样的人，你就是什么样的人。如果你坚持相信自己是一个遭受可怕疾病的无助受害者，而你的救赎掌握在极少数大公司和当权者手里，那么无尽的统治压迫就将是你终生的现实。

你想要什么？

量子物理学告诉我们，我们是宇宙的共同创造者，仅仅观察一个物体的行为本身就会改变其本质，而我们的“主观”意识在现实中扮演着比大多数唯物主义者所想的重要得多的角色。我们对“现实”与自我的认知，更多取决于我们的精神环境（“矩阵”），而非任何唯物现实或遗传倾向。倘若我们能突破文明构建的思维框架、如果能超越这些束缚，万物皆有可能！

> 人类对自身本质与力量一无所知。即便是对自身局限的认知，也建立在过往经验之上，而每一次进步都在拓展人类的疆域。因此，我们没有理由为人类可能成为的模样或可能实现的成就设定理论上的界限。
> —— 英国诗人阿莱斯特·克劳利

如果我们在这个星球上只有一次生命，而又有如此多的待探索、待体验与待发现的事物时，为何要虚掷光阴去迎合这个疯狂社会日益苛刻的期待呢？

[image]

改变总是来自下方，当我们不再依赖旧的压迫结构时，它们就将不可避免地崩塌。

到那时，我们将最终能够创造一种多样性和团结的新文化，

每个人都因其本来的面貌而被接受（和被爱！）。

好消息是：我们通过行动推动的社会变革，对自身生活的影响力，远胜于任何居家疗愈！这并非要建立新的专业阶层来教人们如何生活——这恰恰是我们反对的；正如教师对学生的权威地位会阻碍真正的教学，治疗者的权威也排除了真实的疗愈。有效的疗愈是平等的，个体在相互疗愈中共同成长。

“只要还有人不自由，我们就没人是自由的” 这句箴言，在当下压抑的时代显得格外真实。若不改变环境、不重构现实的根基，我们就无法寻得真正的喜悦与完整。因此，任何深刻的疗愈，必然包含对整个世界与社会的治愈性变革。

列表

[image] 心理健康训练手册：心理安全S08E01

[image] 互助、创伤和复原力：心理安全S08E02

[image] 应对创伤：心理安全S08E03

[image] 走出绝望：心理安全S08E04

[image] 掌控焦虑的策略：心理安全S08E05

[image] 运动创伤的处理和应对技巧：心理安全S08E06

[image] “没有未来”的未来：沮丧，左派和心理健康的政

治 - 心理安全S08E07

[image] “你若盛开蝴蝶自来”、“谁痛苦谁改变”、“接受你永远不会被爱的事实”… 自助文化的愚蠢流行及其威权主义本质 - 心理安全S08E08

[image]
[image]

心理健康训练手册：心理安全 S08E01

[image] 关键词	互助 共生 心理健康 整体安全 疗愈社区
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月2日
[image] **Description**	心理安全

我们期待你不仅将这些工具用于自身，更要施以援手帮助他人。互助是整个过程的重要环节。通过帮助他人，许多人发现自身能力得到提升，某种意义上也是在助己。

- Table of Contents
第一章：引言
互助自助疗法（MAST）的诞生缘由
精神心理健康作为激进的自我防卫
互助自助疗法的认知基础
大脑中的联结：皮层与边缘系统
认知疗法的运作机制
第二章：互助自疗（MAST）概览
综述
MAST的变革流程
第一阶段 - 发现生成信念：打破剧本，创造自发时刻
第二阶段 - 绘制生成信念图谱，构建替代性生成信念
第三阶段 - 用替代性生成信念取代旧有生成信念
完成完整周期后
建立MAST
三人组或团队模式
布局

中间小组分析
第四把椅子
重新集结与项目分析
剧本与自发性时刻
打破“剧本”
挑战与指南
关键考量
第三章：审视我们的信念
信念的生成、中间信念与自动思维
中间信念
模式与灵活性很重要
工作起点：从自动思维开始
识别认知失调
自动思维
认知失调的类型学
第四章：第一阶段
工具、技巧与问题
协作式讨论
节奏把控与适时打断
开发相关主题内容
培养情感与思想的共同语言
厘清术语
“我感觉”、和 “我认为”
触及情感本质
展开缩略语
不仅是语义问题
避免无限回归
从概括到具体（情境）
量表法
运用量表法理解强度或频率
量化以理解改变的意愿
识别认知扭曲
视角工具
俯瞰法
望远镜法
建模
绕道而行
第五章：第二阶段
自发时刻
过渡性问题

1 . “又将如何”？
2 . 直接询问情感影响
3 . “如果并非如此呢？”
过渡性问题的局限性
象征性技术
在三人组中，支持者（或者说第四位参与者）何时应该运用象征性技术？
象征性工具
1 . 开放式绘画
2 . 寓言
如何作为支持者运用象征性工具
第六章：第三阶段
三人组在第三阶段的作用
削弱旧生成信念的力量
主动日记法：
暴露疗法：
信念生成日志：
目标设定：
环境管理：
支持替代性生成信念的工具
替代性日记：
生成信念日志：
强化机制：
重申替代信念：
第七章：MAST疗程之后
复发预防
MAST的结束
1；"我无法独自应对"
2；“我的问题尚未全部解决”
3；"我尚未痊愈"
4；“我还没告诉你真正的问题是什么”
5；"我又开始焦虑了，说明还没到离开的时候"
保持MAST训练成果
自我疗愈
创建情境图式
可视化和日记
自我疗愈的持续支持
第八章：互助与工具运用
结语

 下载本手册电子书： https://z-library.sk/book/0vpbbly8Rr/%E4%BA%92%E5%8A%A9%E5%8D%B3%E8%87%AA%E7%96%97.html?ts=1143

 下载本手册PDF版本： https://mega.nz/file/Gkh3USZQ#kHpBRYIkpyTVrtlro8FFeQgjXmmO5BgAZqMFc4fXZ1I

[image]

第一章：引言

互助自助疗法（MAST）的诞生缘由

"这是人类团结的良知 —— 即便仅处于本能阶段。这是对互助实践赋予每个人的力量的无意识认知；是对每个人幸福与全体幸福紧密相连的认知；是对正义感或公平感的认知 —— 它促使个体将他人的权利视同自身权利。"

—彼得·克鲁泡特金，1902年

简·亚当斯小组的成立，源于激进派活动家对社区心理健康支持的迫切需求。我们选择依靠彼此而非传统治疗或精神医学，部分原因在于：共同应对困境的过程本身，正是强化社群纽带的契机。我们认为这不仅是为解决眼下和长期困境的途径，更是建立亲密互信、坦露脆弱的契机，以此宣告：我们所构建的新社会不应让情感真诚蒙羞。

在创建MAST的过程中，我们的目标始终是帮助自身与他人掌握生存技能 —— 这些终身受用的能力将使我们更加坚韧和健康。

[image]

这正是MAST的自疗理论的核心。

我们坚信心理健康本身就是一场革命。

在压抑疯狂的社会中保持清醒开放的理智，正是对现状可持续抵抗的重要基石。

我们探索新的途径，让社区能够以体现我们理想的方式提供“疗愈”。

MAST不过是这片互助共生生态中的一叶，承载着彼此扶持与责任共担的使命。

MAST是一套开源且不断发展的认知技术体系，旨在通过去等级化的、非病理化的模型，促进个体情绪健康。

MAST 大量借鉴了理性情绪疗法、存在主义心理学、认知行为技术、辩证行为疗法、及相关系统的技术方法。近期我们还引入了符号技术。

MAST的核心在于传授自我反思和解决问题的技巧，助力个体实现情感生活的积极转变。

尽管本质上属于自疗，但**MAST**依托小团体（三人小组或团队）的力量，通过同伴支持，帮助个体运用工具建立自信。

参与者在MAST中轮流担任咨询者与被咨询者，从而全面理解该方法的各个维度。

同伴群体中角色转换的流动性，最终使参与者获得更健康的心理状态，并由此掌握支持他人所需的技能 —— 无论是在我们的激进社群中，还是在更广阔的社会环境里。

MAST摒弃精神健康体系中的传统等级制角色，转而创造更具沉浸式体验的技术理解方式。它同时拒绝现代治疗中支持服务的专有性和专

业主义，鼓励参与者共同完善MAST的理论与实践体系。

MAST既非传统心理治疗，亦非团体治疗。它是在运用互助原则及日益丰富的开源技术体系，帮助人们克服生活中的情感困境。MAST并非替代传统心理治疗与精神医学的方案，亦无意削弱其地位，而是基于更激进的伦理观，提供一种明智的、实验性且有效的自我疗愈方式。该方法虽由心理健康专业人士发起，但致力于与志同道合者共同创建高效支持性实践，以改善我们的精神生活，推动社会根本变革。简言，我们努力将精神与情感的挣扎纳入行动与组织实践的考量范畴。

[image]

精神心理健康作为激进的自我防卫

各类革命者和激进分子投入时间、金钱和精力参加自卫课程，为与国家机器及其他敌对势力发生肢体冲突而做准备，这并不罕见。自卫能力一直是革命事业的重要特征。

然而，身体上的准备只是真正自我防卫的一部分。心理健康作为参与可持续激进事业的必要条件，却常常被忽视。这种疏忽可预见地严重削弱了抵抗行动的效能，同时限制了我们建立的社会关系及创建真正强大社群的能力。

这种忽视源于多重因素：对现有心理健康模式与行业的污名化及合理的质疑，以及资本主义制度下心理健康服务获取渠道的匮乏。

我们必须找到克服这些障碍的途径，探索强化心理健康的方法，以拒绝复制我们所处的暴力体系，并持续挑战种族主义、资本主义和父权制。

如果相信功能失调和压迫性的社会结构只会在物质和身体上影响我们、却不影响情绪和行为，那是很天真的。同样天真的是，相信那些直接受益于这些不公正和压迫性社会结构的精神健康模式，竟能为激进社区的精神自卫和健康提供最佳建议。

压迫性社会屡屡以“心理健康”之名胁迫甚至惩罚反抗统治与胁迫的人们，革命者对心理治疗普遍持怀疑态度实属自然。我们深知压迫势力惯用武力手段，但这并不意味着我们天生排斥以物理手段实现目标。激进疗法的目标不应是使个体同化于现状，而应让个体重新掌控自身情绪与行为，使其能在社区协作中推进这些目标。

激进疗法必须尊重参与者的政治目标。MAST疗法正是其中一种强调自主性与反权威模式的疗法，它允许个体以他们认为富有成效且令人满足的方式来管理自己的情绪和行为。

激进疗法应致力于创造情境，使人们能够自由地化解影响其建立关系与抵抗能力的情感及行为障碍。治疗不仅限于被动应对既成伤害，更可采取主动性的预防措施，帮助个体为未来的压力源、压迫或困境做好准备。MAST的重点不在修复创伤，而在掌握情感与行为的自主能力，实现有意识的情绪与行为管理。

MAST通过激进政治实践的框架来审视传统的认知疗法技术，从而对其进行解构。该方法摒弃治疗师与患者之间的等级关系及固定角色，代之以一个刻意实现角色转换的学习共同体。

叙述者（接受咨询者的称谓）随时可成为支持者（提供咨询者的称谓），反之亦然，由此构建出更具整体性和平等性的社会关系，这与认知心理学的专家范式形成鲜明对比。

MAST借鉴团体治疗与同伴支持网络的工具，创造社群环境，而非采用包括认知疗法在内的所有治疗模式中常见的传统(医患)双人模式。MAST实践极致透明化：在疗程中使用工具前会完整展示所有工具，参与者既体验运用工具帮助他人，也感受他人运用工具帮助自己。

这种方式彻底消解了疗程过程与目标的神秘感。MAST注重自主性，其工具体系抵制治疗场景中常见的依赖关系形成，通过消除双人模式并构建多元团体结构实现这一目标。

MAST强调依靠社群力量提供支持，而非依赖专家或魅力型个体。该体系向普通人传授工具，使其既能帮助他人，最终也能自我成长。

MAST允许参与群体共同制定项目规范，探索相互问责机制，从而营造开放而亲密的氛围 —— 无需强制性"汇报"的场域。

MAST是免费且自愿的，排除了物质考量与胁迫性财务结构，营造开放氛围以促进探索与精进。MAST是一个开放系统。它追求在每次会话中不断演进变革，拒绝僵化教条的解决方案。MAST以认知心理学为基础，但兼容并蓄地吸纳其他模式与思想的影响。

[image]

与传统心理治疗聚焦个体不同，MAST允许问题定位于多重维度，并持续开展对社会结构的政治分析与批判。

激进批判与思想的注入渗透**MAST**实践的每个维度，使其成为明确的政治实践。

MAST无需大量资金、时间或精力即可轻松复制，

亦无需获得专家或管理机构许可。

MAST并非排他性体系，它只是众多工具集中的一个选项。

[image]

互助自助疗法的认知基础

互助自助疗法（MAST）基于认知心理学原理及认知神经学研究成果。该疗法关注情绪与行为如何从大脑运作转化为个体生活表现。本节将阐释大脑神经机制如何塑造多样化心理状态，以及如何调控这些神经过程。

认知疗法某些基本要素的先驱思想，已在西方哲学传统中得到确认，尤以希腊斯多葛学派为甚。斯多葛学派认为，世界的"现实"次于心灵对世界的诠释。此外，两位尤为著名的斯多葛学派代表人物塞内卡与

芝诺强调：破坏性情绪源于判断失误，而"道德与智慧臻于完美"之人可免于经历不快情绪。斯多葛学派坚信个体能够掌控意志，主张人的情感及其对情感的反应（行为）可摆脱外部环境的束缚。

斯多葛学派的哲学强调主观主动地塑造人的情感状态与行为反应，在1950年代的存在主义者中重新引发关注。战后哲学家们 —— 尤其在法国 —— 面临着解释一个非理性且残暴的世界的困境：为何像德国这样的文明国家竟能实施大屠杀。冷战时期，西方世界深陷“相互保证毁灭”（MAD）的末日战略漩涡。身处"荒诞社会"中，人们如何理解自身生存？对萨特、加缪等存在主义者而言，答案正如斯多葛学派所言：在于自觉转变心智模式。

存在主义心理学与理性心理学汲取了萨特和加缪哲学思想的精髓，并将其应用于心理学领域，尤其是心理治疗实践。

20世纪50年代中期，具有深远影响的精神病学家阿尔伯特·艾利斯博士通过理性情绪疗法（RET）革新了心理治疗领域。受斯多葛学派著作及与萨特友谊影响的艾利斯认为，通过建立新的范式（思维模式），"大脑机制可以被改造"，从而使人能够有意识地改变自身情绪与行为。他拒绝了弗洛伊德精神分析及其他心理动力学方法，主张通过刻意而自觉地运用理性，人们能够改变自身的情感与行为状态。

艾利斯提出著名观点："造成心理创伤的并非人和事件本身，而是对刺激的诠释。" 他主张如果我们改变对事件和人物的诠释，必然会改变我们的情绪状态（进而改变我们的行为）。他的见解和技术直接导致了美国和欧洲的认知疗法革命。

大脑中的联结：皮层与边缘系统

认知疗法是由美国精神病学家亚伦·贝克博士于20世纪60年代创立的一种短期心理治疗方法。该疗法基于认知模型，该模型认为思想、情感和行为相互关联，个体通过识别并改变无益的或不准确的思维模式、有问题行为和痛苦的情绪反应，能够逐步克服困难并实现目标。

要理解思维与情绪/行为反应之间的关联，需要认识两个神经系统：

边缘系统和大脑皮质。

- 边缘系统

边缘系统是一组位于丘脑两侧、大脑皮质正下方的脑结构。它支撑着多种功能，包括情绪、行为和动机。情感活动主要由边缘系统主导。

作为自主神经系统的守门人，它最显著的职责是调控生物体的"战斗或逃跑"反应。

该系统通过肾上腺素及131种以上生化物质激活，负责调节身体对情绪的反应。

当边缘系统被激活时，生物体将经历由化学物质诱导的情绪波动及后续行为。

- 大脑皮层

大脑皮层是人类大脑外层的系统集合体，负责思维、问题解决和模式识别等"更高阶功能"。

我们对世界的认知模式与信念体系均在此形成。

当大脑其他区域接收外界刺激时，大脑皮层会解读这些数据，并根据解读结果在必要时激活边缘系统。

边缘系统可被激活为积极状态、消极状态、或保持待命（中性）状态。每种状态都会向大脑和身体释放不同的生化物质。

认知疗法的运作机制

虽然人们无法在刺激发生时有意识地改变边缘系统的触发机制（因为

这个过程发生得太快），但认知治疗师试图提前改变皮层中发生的分析过程，这样一来，当类似刺激再次出现时，传递给边缘系统的指令就会有所不同。

认知疗法的核心在于促使大脑皮层将对负面事物的分析转化为中性甚至积极的解读（反之亦然，积极解读可转化为中性或消极，这涉及逆向条件反射）。

然而这种机械式方法存在精确度不足的问题。认知治疗师通过聚焦于皮层分析背后的模式、假设及信念，绕开了将行为简化为皮层活动的局限。这使人能够有意识地改变对系列关系性刺激的分析与解读方式，进而影响边缘系统的激活模式。改变信念并代之以替代性信念的能力，使人得以控制那些引发不适且无益的情绪与行为的不适应性神经反应。

[image]

第二章：互助自疗（MAST）概览

综述

简·亚当斯集体启动 MAST 项目，源于我们注意到朋友们需要更直接的、更注重成效且立足于社区的治疗方式，尤其是在反等级制度的背景下。我们希望提供一种不依赖"专家对患者"范式的服务，并邀请人们共同参与创建。经过多次MAST疗程的实践迭代，我们不仅培养了部分参与者来协助后续疗程的开展，更在过程中不断完善了该模式。

开展 MAST 疗程时，我们通常将活动设计为两小时的会话单元。首先通过讲座（展示材料与手册）和参与者对话相结合的方式，讲解认知疗法的基础技巧与理论，介绍可在团体中使用的及个人实践的实用工具，有时还会现场演示相关技术。

经过一个小时的讨论后，我们将分成三人小组 —— 即固定的三人组合（如果包含"第四把椅子"则为四人）—— 来实践所学内容。

成员轮流扮演不同角色，每20分钟轮换一次（每次轮换间隔5分钟进行简要总结）。

支持者（咨询师）的目标是学习如何引导每位叙述者（接受咨询者）更深入地理解阻碍其改变不良情绪或行为的障碍。

支持者协助叙述者：

1. 察觉到自己向他人描述生活时使用的思维脚本；

1. 识别到思维中哪些部分属于"自动模式"；

1. 挖掘可能引发负面情绪的潜在信念。

我们共同努力发掘这些深层的信念，理解其本质，并协作探究：哪些触发点会引发痛苦的表现？由此产生何种情绪反应和行为？这些感受何时出现、如何发生、持续多久？

完成此阶段后，我们将用数周时间来构思更健康实用的替代信念，它可能带来更积极的显现形式 ——由此衍生出更健康的情绪与行为模式。

[image]

最终目标不仅是让我们在生活中感觉更好、更有能力、更少陷入困境，

更要在这个过程中建立更强大的社群纽带。

MAST的变革流程

以下是对MAST三阶段流程的极简说明。每个阶段设有独立目标，达成后方可进入下一阶段。认知心理学中存在若干通用工具可贯穿全程辅助个人成长，另有特定工具则专用于三个阶段中的某一阶段。

第一阶段 - 发现生成信念：打破剧本，创造自发时刻

人们拥有众多生成信念（其中部分相互关联），其影响范围从积极向上到功能失调/破坏性不等。多数人存在看似不受意识控制的情绪或行为，且对有意识的改变尝试免疫。这些负面情绪或行为是潜在信念（即我们所称的"生成信念"）的显现。生成信念几乎总是潜藏于潜意识中，问题根源在于该信念对外部经历或情境的反应机制。识别生成信念需深入剖析其多重维度及其自我强化的思维模式。

在此阶段，三人组试图挖掘支撑功能失调或不良情绪/行为的根源信念。

支持者通过运用多种认知工具和积极倾听，引导叙述者绕开其意识层面的"剧本"。人们借助“剧本”解释世界、自我及情感，这种行为本身并无不妥；然而当我们试图改变行为与情绪反应时，可能正是这个“剧本”（即自动化的内在叙事）掩盖着支撑这些不良情绪/行为的潜在核心信念。

尽管“剧本”是一种有意识的建构，呈现出线性的且合乎逻辑的因果关系，但其背后的生成信念却是无意识的，往往并非基于理性构造，而是由认知扭曲所支撑。

第一阶段的目标在于协助叙述者经历一段脱离“剧本”的体验（我们称之为"自发时刻"），它将揭示导致先前确定的情绪和行为问题的潜在生成信念及其相关的认知扭曲和自动化思维。

第二阶段 - 绘制生成信念图谱，构建替代性生成信念

第二阶段中，支持者运用多种认知工具（与第一阶段所用工具不同，但相关），协助叙述者绘制生成信念图谱。

目标在于理解：

1. 特定的自动思维和认知扭曲如何强化了这一生成信念；

1. 触发该信念的诱因；

1. 该信念的具体特征；

1. 以及最终，该信念及其衍生行为与情绪表现，对叙述者生活与目标的影响关系。

在生成信念被完整映射后，叙述者开始着手创建同样详尽的替代生成信念。

替代生成信念是一种有意识构建的概念模式，其细节程度需与被替代的原始生成信念相当。

创建替代信念时，应考量若按此信念行事将如何改变当事人的人生轨迹 —— 审视其正负面后果（所有替代信念体系皆兼具利弊）。

替代性生成信念必须具体详实，并需考量其与其他人格特质的交互作用。该信念应包含当事人已有的若干强化信念。参与者可借助自己的三人组合作或运用特定的认知工具，创造替代性生成信念，来取代那些导致其希望改变的情绪与行为的生成信念。

第三阶段 - 用替代性生成信念取代旧有生成信念

当导致负面情绪和行为的生成信念被识别，且替代方案已确定后，MAST流程的最后一步便是用替代性生成信念（AGB）来取代旧有生成信念（PGB）。

这一过程需分阶段推进并耗费一定时间。逐步实现PGB向AGB的过渡。两者将在一段时间内并存。

本阶段目标在于强化并习惯化**AGB**，同时切断**PGB**的潜意识强化机制。

正如存在多种简明认知工具用于识别生成信念及构建替代信念，同样存在有意识地替换信念的专用工具。这一部分需在三人组之外完成，运用三人组及自我疗愈课程中掌握的工具。

第三阶段中，支持者作为反馈机制，协助叙述者汇报进展或挫折。本阶段支持者的核心目标是为叙述者提供共情支持与鼓励，助力其完成这一自主引导的疗愈过程。

完成完整周期后

当你成功完成一个完整周期后，这个三阶段过程便会变得更容易（也可以更快地）自我实施。

无论情感或行为问题多么根深蒂固、严重或棘手，相同的改变过程都能奏效。

虽然有些问题比其他问题更容易解决且处理速度更快，但过程本身始终如一。参与MAST疗法的个体无需为每个问题学习新工具或技巧，也无需接受数年"治疗"才能完善该过程。叙述者在三人组中获得一次成功经验后，就可以利用自己在先前会话中掌握的工具，独自着手解决其他问题。

[image]

建立MAST

三人组或团队模式

在MAST过程中，参与者将部分时间用于讨论和讲解新工具及概念。其余时间，MAST小组将拆分成更小的单元，称为"三人组"或团队。

三人组是MAST采用的一种技术，旨在提供支持并帮助个体学习认知工具。三人小组的核心目标是协助个体详细识别其生活中引发情绪及/或行为问题的生成信念。若能在6至8周内达成此目标，小组可进一步协助个体确立新的生成信念（即替代性生成信念）。最后阶段需运用自主工具，用替代性生成信念取代旧有的、不想要的生成信念。

布局

三人组是由三位参与者组成的团体，他们共同经历为期数周的MAST项目。成员们协作提供直接的情感支持，并实践项目中学习的各种技巧。

他们以三角形布局的座位团团围住，其中一把椅子被指定为"叙述者"的座位。

叙述者是三人组中正试图解决情感/行为问题并识别生成信念的成员。其余两人担任"支持者"角色，其任务是运用MAST工具协助叙述者识别生成信念的根源。

在每次三人组会议中，每位成员都将担任15至20分钟的叙述者，接受另外两位成员（即支持者）的协助与指导。时段结束后，成员轮换座位，下一位叙述者开始讲述。然后小组将进行第三次轮换，由最后一位叙述者完成讲述。由此，每位成员将有三分之二时间为他人提供支持，三分之一时间担任叙述者并接受其他两位成员的支持。

这种三人小组模式既加速了学习进程，又为成员们生活中各类问题和心理障碍提供了切实支持。三人结构还能缓解个体独自承担支持责任的压力感。

最后，除实践学习与互助学习的益处外，此模式还避免了客户/治疗

师之间的等级关系 —— 这种关系依赖于支持者与被支持者之间单向的互动。

通过轮换角色使每个人更多地承担支持者角色，参与者将摆脱单纯接受治疗而另一人仅提供治疗的模式。在此模式中，责任由三人共同承担，一个人帮助他人的程度（或更多）与帮助自己的程度相当。

中间小组分析

在每次15-20分钟的环节之间，参与者转换角色前，必须留出时间分析刚结束的环节。

通常做法是请刚完成环节的叙述者进行反思，讨论工具的使用情况，进行情绪检查，并审视潜在摩擦点：如对支持者提问或回应的防御性或抵触情绪。

但需谨记：分析并非为了追究过失、归咎责任或提供建议，其核心在于指出有效工具的应用，并提升成员间的互助支持质量。

第四把椅子

如果小组有兴趣，可选择实施MAST三人组的扩展环节 ——"第四把椅子"。

在叙述者身后、三人组物理三角区域之外，可设置"第四把椅子"。虽然三人组无需此角色也能运作，但第四把椅子由已完成**MAST**培训并掌握工具应用的引导者担任。

[image]

第四把椅子的职责包括：协助支持者化解困境、引导会后分析、掌控时间节奏。

后续章节将对此角色展开详述，需特别说明的是：近期MAST实践中已尝试轮换第四位促进者的角色 —— 正如叙述者与支持者角色轮替机制那样，三人组成员亦可轮流担任促进者一职。

重新集结与项目分析

当每个三人组完成工作后，所有MAST参与者将重新集结。

回归大组后，参与者将讨论分析过程中提出的问题、普遍性议题与洞见，以及可为MAST项目增添价值的具体困难或成功经验。

最后需谨记：**MAST**不仅是学习的时刻，更是创新与改进的契机。每个三人小组都是实验场，都可成为持续改进**MAST**项目的契机。

[image]

剧本与自发性时刻

在最初几次会话中，三人组成员倾听并探讨彼此的"剧本"。这些剧本经由叙述者反复在内心与他人之间演练，形成了一套包含未被察觉的认知扭曲和偏见叙事模式。

每个人都在使用“剧本”，它们通常具有实用性和健康性。“剧本”通常包含对听众而言合乎逻辑的叙述，往往保持中立或看似客观。“剧本”也倾向于重复特定观点、短语及概念。

通常，“剧本”能相对轻松地表达出来，伴随着放松但生动的肢体语言，包括眼神交流。“剧本”本身并无虚假或本质错误之处。所有事件或情境都必须经过我们既有的认知框架或模式，以及随之而来的偏见。这仅仅是一种默认行为。

另一方面，在复述剧本中的事件时，其中嵌入的认知扭曲可能会阻碍叙述者看到背后的生成信念和图式。这些扭曲会对行为和反应产生负面影响，因为人们无法充分反思近期经历，从而难以评估未来应采取

的行动。

支撑我们“剧本”的认知扭曲往往 深受社会有毒制度的影响 ，其根基更蕴含着 胁迫与暴力的意识形态 。

打破“剧本”

使用MAST工具的目标之一，是引发自发性时刻 —— 即对无意识信念体系产生更深层的"去剧本化"的理解，该体系正是催生叙述者想要改变的情感和行为特质的根源。

尝试诱发自发性时刻常被称为"打破剧本"。

打破剧本与自发性时刻紧密相连，二者往往依次发生或相继出现。

自发性时刻出现之后往往迅速退回剧本，要努力捕捉。

在三人组互动中，自发性时刻的迹象可能包括：

- 肢体语言变化：活力减弱和/或不再放松；
- 眼神接触变化：例如眼神转向一侧或看向地板；
- 语调与语流中断：例如出现较长时间的停顿或语调显著下降；
- 情绪线索：例如眼眶或皮肤潮红；
- 使用意外隐喻：例如“我感觉自己被埋在沙滩里了”；
- 以及，突然使用情感化、负面色彩浓重的词汇：例如：绝望、狂怒、内疚等。

经过一段时间的三人组会话练习，支持者将更容易识别这些往往微妙的变化。这些瞬间是叙述者开始识别潜在生成信念的窗口，也是支持者运用特定工具与技巧的契机 —— 这些方法能协助叙述者阐明并审视那些未曾被察觉的信念。

挑战与指南

自发性时刻有时难以激发，要"打破剧本"可能需要多种工具和时间才能使其浮现。根据叙述事件或情境的人的不同，“剧本”可能简洁或简单，也可能充斥着冗长的背景铺垫、华丽的细节和旁白。

由于“剧本”如此自然，支持者本身常会被其细节所吸引，从而分散对 MAST 工具的注意力。

此外，若讲述者具备卓越的叙事能力，在“剧本”中增添的细节、氛围乃至幽默元素，都可能分散任务焦点，甚至占据大量治疗时间却未能产生实质成效。

MAST工具旨在收集关于情境的恰当证据、厘清受助者的情绪与用语，或最终打破“剧本”。由于“剧本”看似自然，支持者在三人组互动中的行为可能显得不自然。因此支持者理解一些基本指导原则非常重要，这些原则有助于澄清发现生成信念的过程。

关键考量

- 出勤率

首先必须指出，建立信任、情感支持与共同学习需要严肃认真的态度和坚定的承诺。因此，参与者应出席所有课程，以维持基本的连续性 —— 如果缺乏连续性，就会阻碍在相对短暂的相处时间内建立信任与团队凝聚力的进程。

- 切勿提供建议

在三人组会话中提供建议往往会适得其反，因为其核心目标在于引导叙述者自主识别生成信念，并探索解决其关切/问题的最佳路径。

提供建议可能会导致支持者与叙述者之间产生反效果的互动，同时削弱受助者的自主性。

改变本就艰难，而自主制定的行动方案更易成功。

三人组会话旨在营造平等协作的氛围，而建议的提出可能危及这种氛围。

- 搁置同情心

搁置同情心不应与缺乏同情心混为一谈。

同情心容易导致误解他人的问题，或因将其与自身感受经历联系而产生主观臆断，使问题个人化。同情可能让你误以为理解了实际并不了解的处境。

我们应当给予叙述者支持与鼓励，而非同情。

- 打断

支持者的主要职责是运用特定工具介入“剧本”，推动进程发展。

三人组会话刻意保持短时长，旨在激励支持者及时介入并运用工具加速进程，避免被情境细节分散注意力。因此适时中断至关重要。

这并非意味着完全不允许沉默时刻，或要求支持者停止倾听。

[image]

适宜的中断时机包括：叙述开始重复时，或相关信息沦为无关细节之时。

- 关注情绪/行为，而非情境

支持者运用工具时，需将焦点集中在叙述者的情绪/行为困扰及其潜在信念上。

重点不在于情境细节。支持者只需了解极少实际事件细节，即可有效运用MAST工具。

情境的细节可能会导致注意力从生成信念和自发性时刻上转移开。

- 识别并把握自发性时刻

当自发性时刻的征兆出现时（不同人可能展现不同的征兆组合），请牢记于心。

当事人往往会迅速（无意识地）回归预设的“剧本”模式，此时你可能需要引导他们重返那个瞬间。

此时应运用聚焦于该事件的工具。

- 识别阻力

阻力（治疗术语中通常称为"阻抗"）可能出现在治疗过程中，表现为叙述者角色的人似乎在与自身目标或支持者本身对抗。

一旦识别出这种行为，且当事人愿意探讨时，往往能为后续学习提供丰富的素材。

如果支持者察觉到阻抗的存在，应向当事人指出。

若阻抗持续，应允许叙述者继续表达，同时另辟治疗路径。

请切记，三人组会话 并非 审讯或忏悔场合。

- 不要预测生成信念

支持者不应试图替他人识别或描述生成信念。同样，避免猜测或暗示生成信念可能是什么或不是什么，也是良好的实践。

- 不要假设你理解情绪或行为词汇的含义

我们的语言有时相当模糊，大多数人在描述强烈情绪状态时会使用简单或含糊的术语。支持者应运用专业工具厘清这些词汇或概念的内涵，而非妄断对方意图。

当当事人声称对母亲"愤怒"时，支持者无从知晓其背后真实的情感与行为模式。

[image]

关键在于协助叙述者精准定位所指对象，

甚至需要帮助确认所用词汇是否恰当地描述了该现象。

- 保密性

MAST不依赖法律契约、职业道德委员会及其看似提供的虚假安全感。

[image]

在激进心理健康实践的语境中，保密性可被理解为关于隐私的行为规范、敏感意识与前瞻性考量，这些要素共同构建参与者间的信任关系。

基于此，整个团体及每个三人组都应共同探讨并确立保密性的具体内涵及其践行方式。

常人眼中理所当然之事，于他人 未必 如此，这在涉及到隐私和保密问题时也一样。

三人组并非忏悔室更不是审讯室，每位成员皆可自由考量并遵循自身对隐私的诉求行事。

维护保密性的责任由个体、每个三人组及**MAST**团体共同承担，责任均等。

为了帮助我们思考如何负责任地处理此事，并表达诉求与顾虑，整个参与者团队及每个三人组都应讨论以下问题：

1. 保密范围涵盖哪些人？

1. 哪些信息应属保密范畴？

1. 哪些信息仅限三人组内部保留；

1. 哪些信息需在三人组重组时提交全体小组分析；

1. 哪些信息在MAST之外仍需保密？

1. 三人组何时结束？自疗何时开始？其他社交形式何时启动？

1. 如果感觉保密性出现问题，如何告知他人？

1. 在何种场合或情境下讨论MAST是不合适的？

此项讨论至关重要，是营造严肃互助环境、实现相互扶持的关键环节。

- 建立三人组的困难

根据前文所述，当参与者与叙述者描述的情境不牵涉个人时，**MAST**模式效果最佳。建立三人组的另一关键在于：要诚实地意识到这种理想情况是罕见的。有时我们彼此生活的交织程度，远超治疗所需的理想状态。当参与者来自同一社群时，这便成为关键问题，尤其在小型社群中，参与者往往难以避免深度介入彼此生活。

[image]

组建三人组时，成员应明确：如果与存在既有矛盾者组成三人组，会阻碍疗程进展，或危及隐私安全及其他义务，此类组合不应被强行安排。

作为整体，参与者需接受自己未必是特定三人组的理想人选。

基于此认知，拒绝加入特定组合并非对他人冒犯，而是对治疗工作的尊重，亦符合每位参与者的利益。在许多情况下，与其组建可能弊大于利的组合，不如不组建。

小组应在组建三人小组前共同讨论此事。

若必要且条件允许，可邀请促进者或"第四位参与者"共同商议。

- 如何开始会话

开启会话可能颇具挑战。如果接受支持的人尚未明确具体问题，则需由两位支持者共同引导提问。

可尝试询问对方是否存在特定的反复经历或情绪困扰，希望就此展开探索。这些困扰可以是重大问题，也可以是细微的感受。初始探讨的问题不必过于重大，因为这些问题仅是触发负面信念的切入点，转变信念的进程才刚刚开始。

即便经过第一周的训练之后，开启疗程仍可能面临挑战。人们常遗忘过往疗程内容，或错误认为所有问题已解决。仅凭15分钟的对话，既不可能消除负面信念，也难以根除其引发的各类问题。

支持者可提醒被协助者回顾先前疗程中探讨的问题或主题，或询问过往问题随时间的演变变化。

此外，讨论每次疗程间完成的作业及自我疗愈工具，既是绝佳的开场方式，往往也能提升每次疗程的互动效果。

- 最后

三人组模式并非完美形态，而是一个可持续发展的项目，它能够也应当根据应用场景进行调整。

如前所述，MAST与三人组模型皆属实验性探索，改进既必要又值得欢迎。

MAST并非教条，本身就是一套工具，而三人组仅是其中一环。我们期待每个MAST小组都能在追求心理健康与抗争的道路上勇于开拓。每个团体都有能力为自身及他人发掘新的工具与方法论。这不仅需要学习，更需要信任我们的直觉与创造力。

[image]

第三章：审视我们的信念

信念的生成、中间信念与自动思维

在每次MAST会话中，叙述者将提供一份"剧本"。每次会话的目标就是围绕叙述者提供的剧本展开工作。该剧本是叙述者描述其情感与心理状态的语言载体，将成为三人组主要处理的初始材料。

支撑剧本的信念体系正是MAST需要调整与改变的对象。

该方法的核心目标在于改变信念（或信念体系），进而改造剧本，从而改变由剧本所阐释并过度决定的行为与情绪模式。

在MAST采用的理论模型中，“剧本”被划分为三个相互关联的层次。它们通常按以下顺序呈现：

- 自动化的或情境性的思维；
- 中间层面的主题性的或条件性的思维和信念；
- 最终是生成信念。

生成信念被定义为人们对自身、他人、世界及/或未来所持有的基本、僵化、绝对且普遍化的信念，这些信念似乎会催生并支配其他思维。当生成信念存在不准确、无益和/或评判性时，它将深刻影响个体的自我认知、效能感，并助长对有害行为的选择。

生成信念通常源于"我是"的陈述（如"我是不受欢迎的"、"我是不称职的"、"我被困住了"）。当人们识别出无益的生成信念，并与支持者共同运用认知疗法策略，建立并接纳一套可行且有益的替代信念体系时，才能实现持久而显著的改变。

在认知疗法中，生成信念的挖掘与修正远比情境性思维或其衍生的自动思维更加困难。这类信念通常源于个体成长期（多为童年，有时亦为成年重大压力时期）持续接收的信息。部分人因遭受同伴嘲弄或欺

凌而接收有害信息；另一些人在童年及青少年时期形成适应性信念体系后，成年时遭遇的创伤事件深刻影响了其生成信念。社会、媒体及学校环境同样可能催生不良生成信念。识别生成信念的形成路径，可为干预提供多重切入点。

理解认知理论中生成信念的运作机制，能帮助支持者掌握修改生成信念的工具，并清晰阐述如何运用这些工具实现预期效果。

生成信念植根于更宏大的构念、图式或框架之中。这些框架或图式是过往观念与经验的持久组合，用于有意义地组织新信息，从而影响新观念与经验的感知与理解。换言，图式或框架不仅塑造我们的信念内容，更主导着日常信息处理的运作方式。

中间信念

生成信念是阐释或体现个人认知框架或图式的信念。当图式及其对应的生成信念被激活时，人们会以偏颇的方式体验生活 —— 即 倾向于重视、标记并记住那些更契合自身图式的观念与想法，同时忽略与生成信念相悖的信息。

[image]

因此，框架与生成信念引发的经验偏见存在相互作用：

框架强化个体的生成信念，而生成信念又加剧信息处理偏见。

图式及其对应的生成信念共同催生自动思维与中间信念。

中间信念作为条件性规则、态度和假设（通常未被言明），在人们生活方式及应对困境时发挥着重要作用。它们常以 "如果-那么" 的条件句形式呈现，规定了必须满足的某些规则，以保护个体免受痛苦的生成信念影响。

例如，持有 "我是失败者" 生成信念的人，可能遵循 "如果我所有科目

都能拿A，那我才是成功的" 规则，这被视为积极的中间信念，因其指明了通向积极结果的路径。

但同一人也可能受制于消极的中间信念。不使用条件性语言的中间信念，常表现为对世界运作方式的情绪化态度或假设。这类规则与假设的问题在于其僵化刻板，通常为生活设定无法企及的标准。它们未能考量人生中的意外事件与挑战，必然影响个体达成这些标准的能力。与生成信念类似，它们加剧了强化有害生成信念的经验偏见；反之，经验偏见又强化了这些规则与假设的僵化性。

因此，模式及其关联的生成信念、中间信念和信息处理偏见，在特定情境下催生特定自动思维的现象并不令人意外。处于相似处境的人可能产生截然不同的自动思维，这种差异源于他们拥有不同的生成信念和中间信念体系。信息处理偏见只会进一步增加人在压力或挑战情境中产生负面自动思维的可能性。当这些思维被激活时，又会反哺这些偏见。

模式与灵活性很重要

人们并非仅拥有单一框架或图式，也不仅仅持有单一生成信念体系。相反，人们往往拥有多个图式系统、生成信念、中间信念、自动思维及偏见，这些要素被整合进更宏大的模式中。某些模式影响我们处理生存与稳定等生活必需事务的能力，另一些则影响建立满足关系的能力。还有些模式影响日常或特定活动，如阅读、写作和驾驶。但有害的信念体系可能对人生各个领域造成破坏性影响。

处理生成信念在修正信念系统中起着重要作用，旨在为一个人生活的规则和假设增加灵活性和自主性。由此期待这种弹性能减少有害思维在压力情境或挑战性处境中自动浮现的概率。增强信念体系的灵活性，既能减轻有害模式在不同情境下运作时的负面影响，也能降低经验偏见的极端程度。

工作起点：从自动思维开始

虽然有些人能迅速识别生成信念，但多数人需要时间才能辨识并着手处理。部分人难以识别与负面情绪相关的认知，因此需要先练习处理更易捕捉的自动思维，才能感知其底层的生成信念。另一些人则认为阐述生成信念过于威胁性且痛苦，通过先处理情境性或自动思维建立安全感，再逐步聚焦于中间层或基础信念更为适宜。

基于上述原因，多数工作流程始于情境性或自动思维，继而转向寻找生成信念。当支持者在多次会谈中协作时，如果优先聚焦情境性或自动思维，可通过多种途径警惕生成信念的存在：

1. 例如，引发强烈情绪的自动思维本身可能就是生成信念，或直接体现了生成信念。

1. 长期系统性追踪自动思维的人，能逐渐识别出自动思维或情境思维中的主题模式，这可能揭示该思维背后生成信念的本质。

1. 当当事人自发报告反复出现的、与过往经历相似的体验时，支持者可借此机会梳理这些体验的关联线索及其内化的信息 —— 二者皆可能映射出一个或多个生成信念。

识别认知失调

我们的心理“剧本”中的组成部分并非尽皆有害；其中包含许多有益的、合理且适应良好的思维模式。这些适应良好或中性的思维并非MAST疗法的目标。MAST针对的是与痛苦行为及情境相连的思维 —— 叙述者在某种程度上已认同这些思维对其无益。这类思维往往源于错误、扭曲或未经检验的消极思维模式。我们首先需辨别哪些思维模式会引发不良情绪或行为。我们将从识别常见的思维扭曲与错误思维模式入手，这些模式往往会导致不良行为或困境。

自动思维

理解我们思考事物的方式，对于理解我们如何感受以及感受什么至关

重要。

许多时候，当思维是消极的时，我们就会将其视为“真理”，而实际上这些想法往往不合逻辑，并引发消极情绪。如果能养成识别自身思维的习惯，我们或许就能看清这些思维与负面情绪之间的关联。如果能做到这点，我们便踏上了用有益而非有害的思维取代消极想法的道路。

人的思维本质上是可经现实检验的假设或推测。真正令我们不安的并非思维本身，而是我们赋予这些思维的意义。我们常陷入 "既然我这么想，那必定属实" 的思维陷阱。当善于察觉思绪后，下一步便是：审视这些想法的合理性，并为自己提供更理性、平衡、开放的替代视角。支持者可运用数据收集与反证工具（后文将详述）协助当事人质疑自动思维的有效性。

应对负面自动思维的目标在于识别、审视与替换。如果叙述者无法"捕捉"负面思维，便无法审视和挑战它们。初期独自完成这点往往困难，因此支持者在帮助叙述者发现这些思维方面扮演着重要角色。

即便叙述者意识到思维是消极的，仍然经常会因认知偏见与扭曲而坚信其合理性。支持者的核心任务是引导叙述者质疑这些未经审视的假设 —— 而非直接提供答案。

[image]

认知失调的类型学

- 过度概括

用"总是"或"从不"的表述将单一事件泛化为普遍规则。例如因一次失误就认定自己毫无希望。

- 心智解读

在缺乏实际证据的情况下，妄自揣测他人的想法。常见表现是认定他

人认同自己对自身的负面评价，却未见对方任何佐证言行。例如："我能感觉到他们觉得我很烦人。"

- 夸大与过滤

人们倾向于相信负面的细节，过滤掉所有积极信息。

- 非黑即白的思维

例如当叙述者的表现未臻完美时，便认定自己彻底失败。

- 灾难化思维

人们常过度预估灾难发生的概率，同时低估自身的应对能力。例如："要是被逮捕了怎么办？这会毁掉我的人生。"

- 归因于己

当叙述者认为他人所有言行都是针对自己时。这包括通过比较来判定谁更投入、更聪明等。例如：他人称赞某人才能时，叙述者便会陷入自我批判。

- 归咎于人

将痛苦归咎于他人，视自己为受害者。叙述者常感到无法改变现状。例如："她让我感觉糟透了"、或"要不是她那样做，我不会那样反应"。

- 自责

感觉对周围每个人的痛苦或幸福都负有责任。

- 僵化思维

奉行一套关于自我与他人行为的不可动摇的规则。亦称"童话思维"，即叙述者为生活设定了一套非常理想化的预期蓝图。

- 自证预言

即使在负面期望尚未发生之前，就被接受为事实。预期某种结果通常会成为自我实现的预言。

[image]

第四章：第一阶段

工具、技巧与问题

这些工具既用于每次 MAST 小组会话的框架内，也以调整后的形式应用于参与者进行自我治疗时。

MAST工具按阶段分类。

第一组工具用于处理所谓的"剧本"：即未经审视的认知内容（描述与细节）、情境性思维、认知扭曲以及正负两面的自动思维，旨在逐步识别产生信念的根源。

作为过渡阶段，第二阶段以过渡性问题开端，最终通过绘制图谱来描述、叙述并外化已识别的信念。

第三阶段技术则用于修正并替换生成性信念。

除了这三个实用阶段外，整个过程还需关注关键要素：首先，尽管工

具按阶段划分，但可贯穿全程使用，且阶段推进并非线性，常需往返调整。其次是 "自发性时刻" —— 在MAST过程中随时可能出现。最后需注意的是，工具运用具有流动性与即兴性，本质上是平等对话的体现。尽管工具以对话形式呈现，但其本质区别于日常谈话，需要逐步适应。

协作式讨论

MAST本身并不关注纠正叙述者“剧本”中的错误。“剧本”内容大多与理解叙述者的情感反应、其对自我、他人或世界的信念，以及这些信念在特定情境中的表现无关。

因此，支持者与叙述者通过协作对话与探究，仅针对剧本的特定领域展开梳理，以实现以下目标：

1. 发展相关性内容。

1. 收集数据/证据。

1. 达成关键词汇与核心概念的共识理解。

1. 逐步厘清"生成信念"。

在协作式讨论中，支持者担任引导者角色，协助叙述者：将对话聚焦于关键领域（即便可能引发不适）；理解正在发挥作用的认知假设和偏见及其与特定情绪状态和行为的关系；以及描述生成信念。

MAST团队成员力求保持直接、好奇且开放的态度。讨论由支持者真诚理解叙述者视角的求知欲驱动，而非预设答案的敷衍式好奇。

提问应采用激发思考、提升觉察的方式，而非要求唯一正确答案（例如分别使用 "你知道为什么你对批评反应这么强烈吗？"、而不是 "批

评让你觉得自己不如他人，对吗？"）。

开放式提问还能让叙述者自主作答，而非依赖支持者可能提供的解读 —— 后者会让叙述者感到必须妥协迎合支持者，毕竟认同比反对更轻松，也避免显得不知感恩或难相处。如果叙述者认为自己处于"妥协位置"，便可能不愿透露更多有助于理解问题的想法。

以最直接的方式提问，往往能有效激发负面自动思维。例如："你知道当时被要求接手重要项目时，究竟是什么想法让你如此紧张吗？" 这种提问方法能迅速判断叙述者当下是否具备识别此类思维的能力。支持者应通过清晰具体的问题而非模糊漫无边际的提问来引导叙述者进行内省。虽然复述故事中的基本事实能给予肯定并让叙述者感受到被倾听，但过多纠缠细节或索要更多信息反而会浪费时间，甚至使工作偏离轨道。

节奏把控与适时打断

支持者应警惕对叙述者看似无法回答或回答困难的问题反应过快。这种过快反应往往源于支持者对长时间沉默的尴尬，或对叙述者语速缓慢的不耐烦。但反之亦然。出于礼貌或对支持者身份的不确定感，无论好坏，这些因素都可能阻碍我们及时提出相关问题。我们应保持积极倾听，同时接受被提问打断的情况 —— 即使尚未完整表达。

这类协作式讨论对 MAST 至关重要，需要大量练习才能熟练掌握。此外，过程中协作至关重要 —— 虽有目标导向，但达成路径可灵活调整。

[image]

谨记：MAST既非调查室亦非辩论场。

若讨论陷入循环，则需启用不同工具，此类情况可在会后分析环节探讨。

秉持协作精神，三人组即可推进至下一阶段：开发相关主题内容。

[image]

开发相关主题内容

在确定哪些内容具有相关性并值得探讨时，可能会遇到困难。所有参与者都应主动反思叙述中的特定内容是否具有相关性。在MAST疗法中，反复出现的负面内容（负面想法、感受和问题）是叙述者和支持者首先需要辨别和探讨的相关内容类型。这是因为这类内容最易被察觉，且通常源于负面信念的产生。这并不意味着叙述者呈现“剧本”时只会提供此类内容。

叙述者讨论问题时常呈现混乱状态（情有可原），无法清晰区分情境、想法与情绪。支持者应迅速从情境细节与背景转向情绪与行为：叙述者在事件发生时或之后有何感受？表现哪些不同寻常的行为？

叙述者常在初期对话中寻求解决方案，这应予以避免。支持者必须提醒对方：首要任务是理解情绪，方能探索替代方案。

对话初期阶段的数据收集至关重要。支持者（以及叙述者）收集的数据重点不在事件情境层面，而在于情感层面。情感词汇往往含义模糊，支持者需通过提问厘清具体所指。为此有多种方法可用。

此类提问可能引发三人组的不适感 —— 因问题看似过于直白，但支持者应提醒叙述者：这些提问旨在厘清情感本质及其对生活的实际影响。部分叙述者可能因这类问题产生抵触情绪，急于按既定脚本推进。此时支持者需再次提醒：对叙述者显而易见的事物，对他人而言可能充满困惑。

在初期会谈中，支持者与叙述者通常难以超越识别几个自动思维和认知扭曲的阶段。这项工作虽具价值，但主要作用体现在第二阶段。对话的核心目标是捕捉那些能引向生成信念的自发时刻。

通常第一步是区分叙述者描述的负面内容中：哪些是可被证实或观察的事实（事件与情境），哪些是主观的思考、感受或解读。简言之，即区分客观要素与主观臆测。例如：

- 已证实 – “我的伴侣告诉我她在出轨。”

- 已观察到 – “我看到我的伴侣在和我的朋友说话时多次触摸她的肩膀。”

- 推测或诠释 – “我就是知道我的伴侣在出轨。你知道那种确定自己是对的感觉吗？”

支持者需要强调上述每类内容的局限性，以及将其认定为"真实"可能引发的问题。例如，有人仅凭对所见行为的解读或模糊感觉就指责伴侣出轨，可能导致关系危机。在区分这些内容类型后，支持者可进一步追问：那些被证实或观察到的内容，如何与叙述者的思想情感产生关联？此举旨在区分外部事件与内部感受/思维，为叙述者做好准备，并有望促进后续会谈中更有效的沟通。

有价值的对话需探索叙述者的内在体验与信念 —— 他们如何形成对自我及世界的认知，又如何为事件赋予意义。因此，对内容进行分类有助于团队识别并理解“剧本”与外部事件、个人体验或情绪波动之间的关联。因此支持者需在叙述者剧本的外部世界与内部世界间不断切换，试图揭示公共事件背后的私人化意义 —— 这通常正是痛苦的根源。

[image]

MAST疗法通过区分事件解读、事件本身及情感反应，为心理挣扎创造空间；若要使叙述者受益于MAST，建立这种关联至关重要。

在厘清事件本身与解读差异后，从“剧本”中提炼有效内容的关键环节在于：建立清晰且双方认同的事件描述语言体系 —— 切忌天真地认为所有人描述情绪或心理状态的方式都相同。因此，精确而审慎的语言运用成为触及核心问题的关键所在。

培养情感与思想的共同语言

厘清术语

厘清术语的实践有助于支持者和叙述者共同关注语言的不精确性 —— 无论是描述自我时，还是描述问题时，语言本身都存在这种不精确性。

例如，当某位叙述者提出的优秀项目方案遭他人否决时，他可能宣称："因为他们不喜欢这个方案，所以我就是个彻头彻尾的蠢货。" 此时支持者可追问：究竟什么才构成“蠢货”？或请对方描述“蠢货”的特征？进而探讨：这种对蠢货的定义是否真正符合自身？或方案被否决多少次才算"蠢货"？

“我感觉”、和 “我认为”

在句子中插入“感觉”一词，并不能使句子变成表达感受。人们常在实际表达“我认为”时使用“我感觉”，例如 “我感觉我和伴侣正在慢慢疏远”。如果频繁纠正他人误用“我感觉”的表达，可能会惹恼对方： "当你说'我感觉我和伴侣正在慢慢疏远'时，你真正想表达的是'我认为我和伴侣正在慢慢疏远'。" 然而在MAST疗法中，这类调整至关重要（但需避免频繁或居高临下的纠正），因为修正功能失调的思维能缓解痛苦情绪；因此叙述者必须学会区分真实的思维与情感。此外，若未能做出这种区分，叙述者会误以为自己的"感受"受到质疑，而实际上被指出需要审视的只是他们的思维。

触及情感本质

当叙述者用超过一个词来描述感受时，往往是在描述某种想法。例如，叙述者可能说 "我觉得自己永远无法克服这个问题"，支持者可将其转化为"你产生了'永远无法克服这个问题'的想法"。"当你怀着这个想法时，感觉如何？" 叙述者可能再次用"感觉"开头回应："我觉得治疗帮不了我。" 支持者此时可指出叙述者已表达了两个想法，并再次询问这些想法引发的情绪："沮丧。"

关键在于叙述者要与自身想法和感受建立联结，例如"我永远是个失败

者"或"没人喜欢我"，而非用非个人的语气疏离自己："在这种境遇下谁都会失败"、或者 "人生中总会有人觉得自己不受欢迎"。

展开缩略语

但情况也可能相反。某些叙述者可能仅用单个词语描述情绪，比如"糟糕"、"烂透了"、"特狗屎"。遗憾的是，这类单词描述虽生动，却未能精准定位支持者所关注的情感。

通过询问叙述者的想法（例如 "我在挚友需要时辜负了她；她总是支持我；我表现得非常糟糕"），并追问行为细节（如 "我正用各种方式努力弥补她"），支持者便能将叙述者"糟糕"的情绪解析为内疚 —— 叙述者违背了自己对挚友应尽的道德准则（"我本该像她支持我那样永远支持她，可她遭遇重大困境时我却缺席了"）。叙述者可选择使用"内疚"一词，或保留其特有的表达方式。

某些负面表述可能"仅由电报式简短词汇构成：'孤独...病了...受不了...癌症...没救了'。一个词或短语便能标记整组痛苦记忆、恐惧或自我责备。" 正如疑问句式，电报式表达的负面思绪同样难以剖析回应。例如：因求职失败而愤怒的叙述者，声称自己生气是因为这种处境 "太典型了"。支持者可能自行揣测"典型"的含义，但由于该词存在多重解释，获取完整句式更为妥当。例如叙述者可能因这种情况总发生在自己身上而沮丧，也可能因雇主惯于吊人胃口却不提供工作而愤怒。由于愤怒根源截然不同，支持者需追问"典型"的具体含义或成因。

不仅是语义问题

某些叙述者或许会抱怨定义术语不过是玩弄文字游戏（例如"换几句漂亮话就能让我感觉好些，是这样吗？"），但实际上这具有极其严肃的意义。用"失败者"、"没用"、"没价值"、"没出息" 等词定义自我，不仅是危险的概括 —— 更无法准确捕捉自我的复杂性与独特性。语义精确性能帮助叙述者清晰准确地描述事件（例如"我已两次驾驶考试失败"）及应对方案（例如"我将第三次尝试"），而非聚焦于自我认同（例如"我完全没用。现在干脆放弃算了"），这种思维会阻碍他们从错误中学习，限制自我发展 —— 比如在挫折面前缺乏坚持。支持者

需要通过要求叙述者定义术语来保持他们的警觉性，而不是默认术语含义已被共同理解和接受。

避免无限回归

但必须注意，支持者切忌沦为"意义狂热者"（即不断追问叙述者所用术语的含义，继而追问叙述者为解释旧术语而引入的新术语含义……如此循环往复），否则将陷入关于意义的意义的无限回归。

这种过程既会耗尽支持者与叙述者的精力，又无法得出任何有价值的结论 —— 例如哪些术语在讨论问题时具有实质意义（如仅评估特定行为或行动），哪些则毫无意义（如评估自我）。

定义术语本身并非目的：它是建立语义清晰度的手段，以便开展更具洞见的术语讨论。这一点在第二阶段也需谨记。

何种内容造成最大伤害？

并非所有负面内容都对对话有益。因此支持者需仔细筛选这些认知倾泻，认真倾听叙述者，精准定位那些"造成情感伤害"的内容。

从概括到具体（情境）

当叙述者笼统地谈论自身问题时，支持者往往难以厘清其情绪，因为问题的具体事例始终难以捉摸。此外，情绪在具体情境中（例如"当我眼看要迟到会议时感到害怕"）比在抽象层面（例如"我担心自己守时不好"）更强烈。基于此，支持者需将泛泛问题锚定于具体情境：

当叙述者自称"我就是个爱操心的人"时，支持者可追问"你目前具体担心什么"。如此便能锁定叙述者担忧的具体事项，而非泛泛讨论"爱操心"的本质。

[image]

量表法

运用量表法理解强度或频率

量表法是获取关键信息及抵御负面思维的常用工具。尽管初看可能令人费解，但量表法能为支持者和叙述者双方提供重要内容。

量表法要求支持者请叙述者对其情绪或想法进行评分并定位在量表上。通常采用"0至10"的量表（"0"代表无强度，"10"代表最强强度）。

关键在于通过行为举例说明"0"与"10"的具体表现：例如愤怒情绪中，"0"意味着行为几乎无变化，而"10"则表现为将椅子摔出房间。此举能产生多重效果。

量表法还可用于衡量事件发生的频率，以及情绪出现的频次。例如支持者可询问：“你认为自己遇到这类情况时，有多大比例的时间会感到愤怒？”；或“这种情况发生后，你多久会感到愤怒一次？”

量表还可用于衡量事件发生的概率或可能性。例如，当要求叙述者使用0-100%的量表评估其对负面想法的认同程度及情绪强度时，这些评分对于共同确定调查的临界点至关重要（例如，低于50%的想法和感受可能不那么重要）。叙述者将自身对负面想法的认同度评为80%，愤怒情绪强度评为85%。这使支持者与叙述者得以针对具体情绪和想法展开深入探究。

但如果某些叙述者因评分过程过于机械而感到厌倦，支持者应中止该程序（叙述者通常无需评分便能识别需重点关注的核心想法与强烈情绪）。

量化以理解改变的意愿

量表法挑战非黑即白的二元思维模式，也挑战叙述者提供矛盾描述的"摇摆不定的"倾向。支持者可先请叙述者将感受置于1-10的量表上，并明确说明1和10分别代表什么。随后可追问：叙述者期望达到的数值区间？阻碍当前状态的因素？以及实现转变所需的具体条件。

量表法是多功能工具，既能为后续工具铺垫，也能为已用工具的后续步骤提供依据。正因其灵活性，量表法常与本节其他工具结合或同步运用。

识别认知扭曲

当人们情绪激动时，常会出现诸如猜心、贴标签和草率下结论等常见认知扭曲或偏见。指出这些扭曲现象并提醒彼此：它们反映了思维模式的正常波动，只有当偏见长期存在或过于极端时才会成为问题。这很有帮助。

例如，一位患有社交焦虑症的叙述者说："我深知自己走进房间时，人们都在想'这人真无趣，还是离他远点'；或者如果他们勉强搭话，也会很快走开，因为心里想着'这个人实在乏味'。"

该叙述者另一关键认知扭曲是全有或全无思维："要么像我这样无趣，要么像多数人那样有趣迷人。" 叙述者难以在两种极端立场间看到中间地带：即人们可能同时具备无趣与有趣的特质。当她学会将更多注意力转向外部环境，而非过度聚焦于自认的缺陷时，就能逐渐发现自己有时对某些人而言确实颇具吸引力，并非所有相遇者都能用所谓迷人的谈吐令她屏息凝神。

部分支持者（尤其是刚接触MAST的新成员）可能错误地认为：一旦在叙述者描述问题时察觉认知扭曲的迹象，就必须立即纠正而非倾听对方陈述。这种过度热心的做法反而会产生不良影响 —— 即对叙述者的思维进行过度干预，这会破坏建立非评判性关系的努力。

相反，随着时间推移，MAST参与者学会关注叙述者的关键言论，以机智的方式回应，掌握恰当的停顿或中断讨论的时机，并总结叙述者

所揭示的负面认知内容。

视角工具

视角工具能帮助叙述者抽离自身处境，将问题外化呈现。这使叙述者得以“看见”那些在既定剧本中可能被忽略的其他可能性。诸如建模、俯瞰法和望远镜法等视角工具，能帮助叙述者区分真实情境与渗透于其“剧本”中的认知扭曲。

在协助叙述者形成合理且经过审视的回应时，应给予其充分的思考时间 —— 这可能是TA首次尝试对负面认知构建建设性回应。放缓思维节奏能让我们既看到自己认同这些观念时采取的心理机制，也能发现可供选择的替代视角。鼓励叙述者以更批判的眼光审视情境，可以有效缓解其痛苦情绪的强度。

俯瞰法

俯瞰法是一种视角转换工具，能帮助叙述者以不同视角审视自身处境，针对特定情境中对自身的负面自动思维或偏见信念，培养中立或积极的应对方式。

与其他视角转换工具类似，俯瞰视角同样能协助叙述者减缓负面自动思维，区分实际情境与自身内心“剧本”。运用俯瞰视角时，支持者会引导叙述者从情境中抽离，以全新角度审视自身思维剧本。

例如：叙述者描述与陌生人开会时的焦虑感，TA认为他人不关注TA的发言且轻视自己。TA找借口离开会议室，认定"别人讨厌我"、并"不该再参加这类会议"。在上述案例中，支持者可询问局外人眼中的情境全貌，并引导叙述者思考：当时采取何种行动更妥当？整体情境如何能得到改善？这使叙述者得以从自身参与时可能忽略的视角审视事件，从而修正即时反应，察觉揣测等认知扭曲带来的影响。

望远镜法

望远镜法和俯瞰法类似，但它用于同时回溯和展望未来，以比较在审视过去或未来时视角如何转变。例如，支持者可能会询问叙述者，他们认为这种情况的负面影响在相对较短的时间内消退的可能性有多大；或者叙述者可能会询问这种负面状况可能持续多久（一周、一个月、一年）。

同样的，另一种望远镜法可询问叙述者：是否曾经历过类似的困境和痛苦情绪？能否设想倘若未来再次遭遇此情境会如何应对？或许当下看似难以承受之事，不久前还觉得无足轻重？；又或许多年前觉得难以承受之事，如今看来不过寻常。

望远镜法的核心在于提醒叙述者：人们常过度评估当下事件的重要性，却忘了过往经历与未来可能的改变。例如：叙述者描述分手后的剧痛，认定"我无法恢复了不会再爱了"、"这份痛苦永不会消散"。

支持者可追问：叙述者是否经历过类似困境？当时如何应对的？这能帮助叙述者意识到：负面影响会随时间消退，并觉察认知扭曲（此处为灾难化思维）的危害。

建模

建模是另一种视角工具，它让叙述者通过获取局外人的观点来将问题外化。支持者可通过提出建模式问题来打破叙述者的固有思维模式，例如询问如果朋友在类似情境中寻求建议，叙述者会如何回应。

支持者可能引导叙述者设想：如果自己站在他人的角度上，会如何探讨自身的情绪、行为及处境。因此，建模提供了一种自我对话模式，让叙述者设想自己会如何为处境相似的亲友提供建议或安慰。

通过建模将问题外化，叙述者得以抽离情境，发现那些可能被忽视的其他可能性。例如：某叙述者因八岁儿子在户外玩耍时受伤而自责。她认为 "如果当时更专注些本可避免"，并自责 "让这种事发生，自己不是个好母亲"。

支持者不必直接劝诫她停止自责，而是运用建模法询问：如果朋友或邻居遭遇同样情况，你会如何劝慰？这能让叙述者自主获得新视角，察觉自身自动化思维中的认知扭曲。

绕道而行

MAST方法致力于挑战那些引发心理痛苦的生成信念。频繁中断有助于揭示心理叙事的漏洞，但并非适用于所有问题。当处理创伤或悲伤时，营造安全的支持性的环境远比审视问题根源的叙事更重要。这类情境中问题往往显而易见：某种可怕的事情发生了。允许自己舒适地体验创伤与悲伤带来的痛苦情绪，能让人学会以更少痛苦的方式面对这些事件及其余波。

创伤与悲伤是生命常态，无政府主义者在反抗压迫性体制时，更可能遭受国家机器或其代理人的创伤。任何针对无政府主义者的心理健康干预方案，若缺乏应对创伤与损失的途径，都将是不完整的。

我们的应对之道是建立安全阀机制，允许灵活切换处理方式，我们称之为"绕道而行"。

假设叙述者向支持者倾诉：自己刚在逮捕过程中遭警察殴打，至今难以释怀。叙述者表明希望畅所欲言不受打断。此时三人组启动绕行机制，叙述者得以在最小干扰下倾吐心声。若叙述者感到舒适，随时可回归常规MAST模式，但选择权始终掌握在叙述者手中。

这种设计营造出安全感 —— 频繁打断往往难以维系的安全感。它更将治疗过程的主导权交还叙述者，使其自主掌控疗愈体验。

绕行机制虽为创伤处理而生，其核心原则却能随新需求与新方法的涌现不断拓展。

[image]

第五章：第二阶段

自发时刻

自发时刻是指治疗过程中出现的语言/情绪/行为变化，往往预示着生成信念的临界状态。这些变化可能发生在每次治疗的任何阶段。

生成信念主要存在于无意识领域（或极少数情况下存在于前意识层面），因此难以通过单纯的意识途径触及。在清醒状态下，意识常会覆盖无意识，使得无意识难以维持较长时间。

支持者需要敏锐察觉这些偏离“剧本”的转变，因为它们是进入叙述者思维的重要切入点。

这些转变可能显而易见（例如突然发怒），也可能微妙难察（例如眯起双眼）。当叙述者以冷静口吻谈论某议题时，支持者如果能察觉其举止间的情绪波动，便可推断为情绪变化。

这类变化被称为"自发时刻"，因其打破了既定“剧本”，且往往转瞬即逝，随后叙述又回归原有模式。

自发时刻常向支持者传递这样的信号：叙述者正从自动思维转向信念生成，此时正是运用过渡性提问（详见下文）的契机。

每个自发时刻各不相同，但存在可供支持者辨识的共性特征：情绪变化、肢体语言变化及语言变化。

- 情绪变化通常表现为反应强度提升，随后伴随与“剧本”常规情绪基调形成反差的释然感。
- 肢体语言变化可能表现为眼神游离、四肢不安分地摆弄，以及叙述者说话时不常见的（基准线外的）其他无意识动作。
- 语言线索可能是偏离“剧本”最常见的迹象，因为三人组模式本

质上是交流互动。异常隐喻、回答前的长时间停顿、语句支离破碎，以及语调音量变化（通常降低）往往伴随“剧本”中断出现。

脱离“剧本”的状态仅持续极短时间。支持者必须通过过渡性提问有效把握这段窗口期。对某些叙述者而言，此时可能伴随强烈情绪痛苦。

强行维持自发时刻毫无意义，当叙述者感到不适时，支持者应允许其返回“剧本”。

当叙述者回归“剧本”模式后，支持者关注并聚焦于较早的自发时刻通常是有用的。过渡性问题可援引先前自发时刻，即便提问时叙述者尚未处于该状态。例如：在先前会话中，叙述者谈及被母亲的期望所“困扰”时曾哽咽落泪。后续会谈中支持者指出，叙述者似乎超越了她惯常抱怨母亲不理解自己的选择的层面。支持者随即可追问她使用"困扰"一词的具体含义。

上述案例展示了支持者如何准备进入过渡性提问，以期阐明并描述潜在的生成信念。支持者必须具备识别自发时刻的能力，方能利用短暂时机启动过渡性问题。

过渡性问题

过渡性问题是一组关键工具，用于帮助叙述者超越具体细节和消极的自动思维，抵达当下的自发时刻。这些问题应在证据收集与澄清性问题之后使用，能将反思引向生成信念及其相关的情感特征。正因如此，它们被称为过渡性问题。

1 . “又将如何”？

当支持者向叙述者提出 "又将如何" 的时候，可促使叙述者反思负面自动思维或印象背后的深层含义。

该问题旨在探究持有此信念的意义何在？这种信念会带来哪些（情感与行为层面的）后果？

此类过渡性问题可能被叙述者感知为具有攻击性、冷漠甚至带有评判意味，故需谨慎使用。仅适用于已经与叙述者建立积极关系的支持者。例如：当叙述者谈及饮酒能让她更容易被周围人接纳时，支持者可追问 "如果不被接纳又将如何？" 叙述者回应称将陷入孤独且难以承受。

在上述案例中，"又将如何" 的问题将讨论焦点从饮酒转向叙述者对孤独的恐惧、及其应对无力感。这使支持者得以探索更深层的情感领域，相比单纯陈述"我喝酒是为了更受欢迎"，这种方式更易引发叙述者的自发时刻。

2. 直接询问情感影响

另一种过渡性提问是直接引导叙述者反思自动思维的情感影响。这种反思对某些人而言可能颇具难度，以至于他们有时会直接改述问题。此类过渡性提问的优势在于直指核心。例如：某叙述者反复提及在各类会议中（尤其男性主导的场合）感到不被倾听。支持者可引导她回溯最近一次遭遇，询问当时的感受：经历了哪些情绪？

在上例中，支持者帮助叙述者与她反复提及的问题建立情感联结。这种联结不带评判，也不暗示她“本应有”的感受，从而能引发更深入的反思，创造脱离预设“剧本”的自发时刻。

3. “如果并非如此呢？”

有时叙述者可能感到情绪脆弱，或潜藏在言语表层之下的负面情绪过于强烈，导致深入探究负面自动思维时会遭遇巨大阻力。这种状态应得到尊重。如果支持者察觉此类情况，可尝试"如果并非如此呢" 的提问法。该问题引导叙述者设想：当自动思维被否定时，自身可能产生的情绪（如果有的话）。这允许叙述者反思一些不那么私人或直接的事情，但仍可能导向实际的生成信念。

例如，当叙述者被要求剖析 "她愚蠢/轻率的行为导致了关系中的言语虐待" 这一自动思维时，支持者察觉到其抗拒情绪。支持者询问：如果事实并非如此，她会如何感受？当与伴侣争执时会产生什么样的情绪？叙述者回应称，她会感到如释重负，不再时刻自我怀疑。支持者回应道："所以现在发生这种情况时，你一定感到压力很大，而且长期处于自我怀疑状态很煎熬吧。"

此类问题既能帮助支持者推断叙述者的情绪，又使叙述者得以保持情感距离避免重温痛苦。当叙述者因自动思维感到羞耻或愚蠢、或感到被评判时，此类过渡性提问尤为有效。支持者随后应该重述相反的情况，以确认方向正确。这是间接获取相同信息的另一方式。

过渡性问题的局限性

熟练运用这三类过渡性问题后，支持者通常能穿透自动思维，直抵其背后的生成信念。实践证明这三种工具最为有效。但参与者需警惕过渡性问题的潜在陷阱与局限。

首先是 "无无尽递归"。即：支持者提出过渡性问题后，获得叙述者的回应，随即又抛出新问题。这种循环可能永无止境，却无法厘清核心生成信念。

关键在于把握何时通过过渡性问题打破”剧本“模式。经验法则是：当情境或表述在不同会话中重复出现时，应及时提出过渡性问题。

第二个潜在问题在于，叙述者可能感到被忽视、或被强行跳过先前的陈述。因此必须与叙述者建立良好关系，并在提出特定问题时保持透明沟通。

此类工具的局限性在于：它们虽能激发瞬间的自发性，却难以维持这种状态。重复使用相同问题可能无法达到先前的深度，此时支持者需转换提问类型。

[image]

尽量使过渡性问题简洁明了；

叙述者的精力应集中于反思，而非费力追随支持者的提问节奏。

总体而言，过渡性问题是突破自动思维表层、触及生成信念的核心工具。如果能有意识地运用并把握时机，它们就能成为最有效的工具，既能引导叙述者开始反思潜在的生成信念，又能推动其进入MAST的第二阶段。

当过渡性问题没能引发自然回应时（可能存在多种原因），可考虑采用象征性技术（详见下文）。

[image]

象征性技术

象征性技术在MAST疗法及心理治疗领域均可成为强有力的工具。

自弗洛伊德以来，我们已知心理问题的根源多潜藏于意识之下，深埋于无意识之中。象征性技术能直接与无意识沟通，加速发现核心信念的过程。

运用象征性技术应视为对MAST其他认知工具的补充，而非替代。

无意识的结构与意识截然不同，它遵循自身独特的规则、语法和序列逻辑，所调动的脑部区域也与意识活动不同。通过普遍存在的梦境体验，我们都熟悉无意识的某些奇异之处。梦境往往高度象征化—— 人物、场景与事物同时承载多重意念、情感或体验 —— 且摒弃了清醒思维的因果逻辑。其隐喻性与非线性结构使梦境难以被意识解读，更因叙事常脱离日常经验与理性思维而易于遗忘。

象征技法的运用分为两种模式：权威式和容许式。

- 权威式使用以精神分析为代表，通过解析他人的无意识表现（梦境、口误、自由联想等），由治疗师或分析师运用分类法和抽样法解读每种无意识表现，并向来访者提供分析。

- 容许式方法则认为每个人的无意识都具有独特性，由个人经历及来自家庭、朋友、社会的期许构成，并运用其专属的象征体系。采用容许式方法时，治疗师试图激发客户的无意识反应供其自我分析，治疗师本人不作任何解释。

为构建符合政治原则的心理健康援助模式，我们在**MAST**中运用象征技术时采用容许式方法。下文将重点阐述MAST三人组运用象征技术的时机与方式。

在三人组中，支持者（或者说第四位参与者）何时应该运用象征性技术？

这类技术在一系列会谈初期最为有效。如果支持者难以通过常规认知工具促使当事人真正识别问题（及其生成信念），尝试象征性技术或许有所助益。如果三人组决定采用象征技术，需提前确定由哪位支持者实施（因其需要不同于传统认知技术的专注形式，详见下文）。

象征技术仅用于创造"自发时刻"，随后支持者将运用认知技术/工具识别并构建替代性生成信念。在MAST流程的后期阶段，象征性技术将失去效用。

此外，象征性工具不应作为MAST会话的首选工具。会话应以认知工具和方法开场，以此激活潜意识对当前问题的关注。当投入一定时间尝试触及问题核心或生成信念后，象征工具方能发挥有效作用。

象征性工具

1．开放式绘画

“开放式绘画”是一种需要纸张和书写工具的技术。

支持者（小莉）先在纸上画出某个物体（通常偏离中心），然后将纸张递给接受支持的人（小强）。小莉要求小强每次只画一个物体，通常要求对方总共画不超过4-6个物体。此外，小莉会要求小强用单个词语标注部分或全部画作。

整个过程中，小强应以遮挡视线的方式持握画纸 —— 事实上，任何时候支持者都不得窥见小强的画作，否则会因主观解读而干扰疗程。

关键在于小莉不应在每次作画间隔给予小强过多时间。整个绘画过程仅需数分钟完成。

绘画结束后，小莉将通过开放式提问引导小强分析画作。此类分析可通过三类问题实现：

1. 第一类涉及情绪状态的问题，例如：画作传递了何种情绪？如果他人（特定对象）看到此画，会产生何种感受？画中的人物有何感受？

1. 第二类问题关注元素间的关系，例如：画中哪个元素最大/最小/居中/最靠近其他元素？两个元素间有何关联（具体而言，元素A对元素B有何感受）？元素在时间维度上如何关联（哪个元素出现得最早或最晚）？

1. 最后一类是超出情境的问题。这类问题引入画外元素，需要推演思考，有时会引发困惑。例如：一小时后会发生什么？你会对其中某个元素说什么？如果这是故事/电影/卡片插图，会属于哪种类型？如果这幅画挂到美术馆里，会取个什么样的标题？

[image]

关于如何有效运用开放式绘画的建议：

首先，要求参与者将自己性别的人物作为元素之一进行绘制。

练习中避免使用"你"或"你的"这类代词。

给出具体元素（如树木，而不是森林）。

为人物添加非特定名词的物品 —— 例如说："给人物添置旅行者会携带的物品"，而不是直接要求"给人物画顶帽子"。

解释你不会查看这幅画。营造悬念氛围，并在任何结论形成前结束绘画环节。

2. 寓言

寓言工具是由支持者（小莉）讲述的故事。关键在于将当事人（小强）在会谈前期使用过的某个词汇，以不同且/或更开放的方式重新运用。例如，如果小强抱怨他人"贬低"他的工作，小莉可讲述一个关于小精灵的故事，将"微小"的概念具象化呈现。

童话、寓言等类似故事结构均可采用。故事需至少包含两个角色且具有开放式的结局（不作最终定论或收尾）。故事时长应控制在数分钟内，通过营造悬念却不提供明确结论，来引发受助者的挫败感。

首要问题通常是："你对这个故事有何看法？" 随后小莉会追问故事相关细节：角色当时有何感受？后续遭遇了什么？角色间存在怎样的关系？这个故事揭示了角色所处世界的哪些特征？如果故事结束后你能遇见这个角色，你会对他说什么？…… 等等。

[image]

运用寓言工具的要诀包括：避免为人物或地点命名，可重复故事中的动作或台词，至少设置一个意外转折，并善用眼神交流、手势及拟声动作（如敲击桌面模拟敲门声）。

如何作为支持者运用象征性工具

如果决定在三人组中使用象征性工具，务必让另一位支持者及接受支持的人知晓。一切应尽可能保持透明，这不会削弱象征性工具的效果。象征性支持者必须采取有别于认知支持者的支持方式。

象征性支持者需练习"不专注倾听" —— 即在不被叙述内容牵引的前提下聆听。象征性倾听关注言语本身，但要忽略其语境和细节。支持者可时而专注时而抽离，避免完整接收叙述内容或上下文。此举至关重要，因为最有效的象征性工具源自支持者潜意识，而非意识或专注状态。

[image]

具体可通过分散注意力实现：如逐字记录、定期走神、故意分心等。

你需要适时打断对方（作为认知支持者你应已具备此经验）。

关键要通过眼神交流快速建立连接，这可能需要调整位置靠近对方、稍提高音量、配合手势，并展现微笑等积极面部表情。

告知对方你想"尝试新方法"，随即启动其中一种工具。

所有工具均需由象征性支持者提出开放式问题。持续提问直至认知支持者介入。当认知支持者感知对话逻辑中断或洞察形成时（通常在五个问题内），应立即终止提问。此时认知支持者接管引导，象征性支持者则回归认知支持角色，转为主动倾听。

每次三人组会谈仅使用一种象征性干预。通常应安排在会谈初期，以便留出充分讨论分析的时间。需提前告知被支持者本次会谈将运用象征性工具。相较于三人组中的两位支持者，第四位参与者往往更易运用象征性支持。当难以突破固有思维模式、问题模糊不清或疑似伪问题、受助者难以识别生成信念时，可考虑运用象征工具。此法能显著加速三人组会谈中的MAST进程。

附录收录了米尔顿·埃里克森博士的实例，可供开发专属象征工具时参考。

[image]

第六章：第三阶段

第三阶段运用MAST疗法中的自我疗愈工具，其核心特征在于用替代性信念取代原始的、令人困扰的生成性信念。在此阶段，三人组的角色会发生显著变化。

第一阶段：致力于揭示自动思维，并鼓励自发时刻。

第二阶段：详尽剖析有问题的生成信念，及其与各类症状（积极、消极、及中性）、环境及叙述者人生目标的交互作用。此外，第二阶段致力于构建同等详尽的替代性生成信念图谱/模式，以替代原有的生成信念。

第三阶段：旨在减少原有生成信念的发生频率及其对情绪和行为的影响，最终实现替代性生成信念的置换。

第三阶段与前两阶段不同，其主要工作并非在三人组内完成，而是在组外进行。

三人组在第三阶段的作用

第三阶段代表了自我疗愈过程的核心环节。虽然仍由一位叙述者和两位支持者构成，但相较于前期阶段，他们的角色定位与运用工具均发生显著变化。

首先，在前期阶段，支持者会尽量克制同情心，并保持客观视角，以此协助叙述者达成目标。而在第三阶段，支持者适度展现同理心并分

享自身经历（如艰难转变、耐心等待、反复复发等），反而更具助益。客观视角并未完全消失，而是与积极鼓励等激励技巧相结合。

明确表达对改变之难的认同和赞赏是这个阶段常见的支持性工具。支持者还需引导叙述者关注其可能忽视或羞于承认的成功。

与其他阶段相似，本阶段重点在于协助叙述者运用特定阶段工具达成目标（如生成信念替代）。例如：叙述者希望用 "自己有能力应对威胁" 的新信念，替代 "自己会遭受攻击"的旧生成信念。

叙述者抱怨参加和平示威时，活动全程顺利，唯独结束时独自一人走向公交车的路上经过一些喧闹的警察时感到了恐慌。支持者指出她能无惧参与示威已属难得，并强调即便是示威结束时遇警察产生的恐慌，不久后也会消退。支持者提醒受助者：情绪与行为的重塑需要时间，而能在游行中不假思索地控制恐惧，已是朝着正确方向迈出的积极一步。

上述案例中，支持者们认可了渐进式进步，并指出叙述者完成整个心理重建过程尚需时日。

削弱旧生成信念的力量

要成功用替代性生成信念取代旧有信念，关键在于削弱旧生成信念的力量。所谓力量，指的是当副交感神经系统启动时，它会强化原有生成信念，从而使新信念更难取代。许多生成信念根深蒂固，因此其抗削弱性相当强。削弱旧生成信念在个人情感/行为生活中的作用往往需要时间。

解决此问题的最有效方式是让叙述者尽可能了解生成信念如何影响其情绪/行为。例如，可识别伴随并强化生成信念的自动思维。简单地识别并标记正在发生的事情，就可以明显削弱生成信念的情感和行为力量。

以下是叙述者可实践的若干工具。

主动日记法：

尤其在初期，旧有生成信念被触发时，往往伴随自动思维的连锁反应及不良情绪行为症状。

当当事人情绪平复后，可客观记录事件经过，着力识别导致不良结果的自动思维、认知扭曲及其他要素。事件发生后立即记录效果最佳。

此工具可单独使用，亦可与替代性日记（见下文）结合运用。

暴露疗法：

许多引发信念的触发因素具有随机性且毫无预警。暴露疗法要求当事人刻意接触有限剂量的触发变量，从而察觉自动思维、认知扭曲、情绪及行为等反应的流动轨迹。

例如，如果叙述者在人群中感到困扰，可选择主动接触小型人群数分钟，随后反思自身感受与行为表现。下次可尝试接触稍大群体或延长停留时间。

此法成功的关键在于：除暴露体验本身外，不附加任何其他要求。

信念生成日志：

叙述者可通过简易的日志作为反馈机制，记录进展并识别信念生成过程中哪些部分更具韧性。

日志应保持简洁，以便事件发生后数秒内完成记录；附录中有提供日志模板示例。

目标设定：

目标设定是削弱生成信念影响力的强效工具。

成功运用该工具的关键在于目标需具备简单、可量化、有时限的特性。

目标应直接反驳旧有生成信念，或支持替代性生成信念。

环境管理：

此处的目标设定原则与前述相似。管理对象应具明确性、简洁性，并聚焦于：减轻症状性情绪/行为的负面影响，或强化替代性生成信念的积极要素。

反思和意向性是所有这些工具以及成功完成最后阶段的关键要素。最终叙述者有望摆脱这些正式工具，在自身心理层面实现同等效果。反思即识别生成信念如何通过特定自动思维与认知扭曲显现，并如何影响事件的情感/行为结果；意向性则指预先规划可建立何种认知框架以改变不良模式。

支持替代性生成信念的工具

叙述者应同时运用这些工具和削弱旧有生成信念力量的工具。替代性生成信念的强度与其试图取代的原始信念呈反比关系。

替代性日记：

此工具与主动日记的区别在于，在事件被记录下来之后，叙述者会重写它，去除自动化思维和认知扭曲，并想象这会给情绪和行为带来什么样的改变。

生成信念日志：

不仅仅记录旧生成信念的自动化思维和认知扭曲，还可以记录与新的替代信念相关的思维。

强化机制：

当实践中察觉替代信念产生影响时，找到一些积极的东西来奖励自己。最成功的奖励是小而渐进的，并且在时间上接近事件。奖励内容无需与替代信念相关联，仅需是个人喜好的事物即可。

重申替代信念：

在此阶段尽可能以多种形式重复替代信念。可大声说出、绘制图画、书写记录、设置为屏保程序、发送短信给自己等等。尽量保持措辞一致。

替代旧有的信念需要时间。这个过程并非线性发展，叙述者应做好心理准备：过渡期可能出现旧有信念看似增强的阶段。如果缺乏耐心或难以坚持，除运用上述工具对抗旧有信念外，还需制定应对策略。替代信念完全生效通常需要3-6个月。成功替代的标志是无需再依赖工具，转而运用反思与自觉性进行自我调节。

信念替代过程中，叙述者常会察觉到其他相关的不良生成信念浮现。这是正常的。关键在于先完成首次替代，再着手处理其他不良生成信念。

[image]

第七章：MAST疗程之后

复发预防

人们能够向更好方向转变，这正是我们进行治疗的原因，但应对复发或倒退的可能性或许同样重要。

复发指完全回归至先前问题状态，而倒退则指部分回归至先前问题状态。

当治疗接近尾声时，参与者将认识到（若此前尚未领悟）：改变并非平滑线性进程，而是前进与退步的交织 —— 其中部分起伏他们已在治疗中亲历。基于此，认为我们能完全预防复发实属承诺过高。

我们更倾向使用"复发风险降低"这一术语，它更准确地描述了治疗后可能面临的进展，毕竟每个人都不是完美的。复发风险降低是一种现实策略，具体做法是：识别可能引发复发的潜在情境（如人际冲突、强烈负面情绪、孤独时刻），并协助参与者制定应对方案。这些方案需运用他们在治疗中已掌握的工具与技巧。

参与者需设想自身处于这些情境中并演练应对策略。这些练习可模拟当下情境而非未来场景进行。

例如，一位参与者坦言与伴侣争吵后可能因难以承受愤怒而酗酒，她便在卡片上写下替代性思维和行为："给 MAST项目的朋友打电话聊聊"； "到家中安静处平复情绪"；"聆听舒缓的音乐"；"前往健身房锻炼"；"强迫自己意识到：我无需酒精来应对困境，决心以清醒头脑直面挑战"；‘待情绪平复后，与伴侣沟通时避免辱骂、自责或吼叫，并为自身不当行为致歉。’

参与者可由此领悟：一次失误（如饮酒或未遵守饮食计划）未必导致全面复发 —— 只要及时应对失误，便不会存在滑坡效应。

应对失误的有效策略与信念包括：

- 接纳失误是进步过程的组成部分
- 从失误中汲取教训以完善未来的应对策略
- 认识到改变并非一蹴而就
- 相信复发是选择的结果（即使选择未必明显或自觉）
- 避免非黑即白的思维定式，例如："酒鬼永远改不了"、或 "既然已经破坏了饮食计划，坚持下去也没意义" 等等 —— 此类想法会增加失误演变为复发的可能性。

复发应对策略帮助参与者理解：失误是学习机会，而非个人缺陷的标志，失误后仍可重新回到正轨。将复发重新定义为学习或自然实验 —— 即参与者在治疗结束后未遵循维持进展的指导方针时会发生什么 —— 有助于他们认识到：失足/复发只是改变过程中的个别事件，而非改变的全部。

MAST的结束

MAST的结束可在课程伊始便予以探讨；可将其定位为一个协作过程 —— 参与者将共同习得一系列自我疗愈技能，这些技能既可在课程期间运用，亦可在课间实践，从而使参与者成为自身问题的解决者，最终以更成熟的自我疗愈能力完成**MAST**课程。

随着参与者在应对困难方面建立信心与能力，后续疗程应仅基于参与者需求继续进行。采用"倒计时"策略颇具成效 ——在 每次疗程中提醒参与者剩余疗程次数，可最大化疗愈效益。

如果MAST的结束方式未经规划或考量，将很可能削弱参与者从疗程中获得的收益。

[image]

因此，确保MAST结束过程高效顺畅至关重要。当MAST收尾处理得当，每位参与者更可能巩固疗效并推广应对未来问题的策略。

可引导参与者总结 MAST 带来的收获，包括他们认为特别有价值的理念和技巧。记录这些收获也颇有裨益。例如某参与者表示："将思维置于聚光灯下，让我真切意识到自己竟是如此极端化思维者。" 她将特别铭记两点：（1）思维通常是假设的而非事实，"因此通过审视就能改变它们"；（2）我们都能自主选择应对方式："参与MAST前，我认为是情境让我愤怒，现在我意识到自己拥有更多选择权来决定如何反应。" 她发现渐进式肌肉放松法（通过系统性收缩放松全身主要肌群并保持缓慢呼吸）极具助益 —— "因为愤怒与放松无法并存，而我更愿保持放松状态。" 针对可能引发持续性暴怒的未来困境，她制定了应对行动方案。

参与者常对结束MAST项目心存顾虑，这些问题需要得到解决。其中包括：

1；"我无法独自应对"

参与者通过完成作业已开始独立行动；此外，我们仍能铭记其他参与者给予的鼓励与支持，因此心理上并不孤立。遇到困难时，他们可进行想象中的咨询对话。

每个参与者都可以通过独自行动将这种预测视为需要经验检验（就像治疗中的所有其他预测一样）。

2；“我的问题尚未全部解决”

MAST并非旨在解决参与者所有问题，仅处理部分问题。参与者在MAST结束后可将自助技能应用于其他问题；如果在离开MAST前就解决所有问题，只会削弱参与者成为自我支持者的理念，并可能导致参与者依赖MAST来解决所有问题。

3；"我尚未痊愈"

重申，MAST从未以"治愈"为目标，而是旨在降低问题的发生频率、强度及持续时间 —— 换言之，更有效地应对问题。

通过在困境中运用MAST技能并从经验中学习，参与者的自我管理能力将日益精进。

4；“我还没告诉你真正的问题是什么”

这种说法可能会给人一种印象，即到目前为止的 MAST 只是探索“真正内容”的序曲，但现在 MAST 已经结束，为时已晚。支持者可以简要探讨参与者为何在最后一刻才透露这个问题，并选择是否延长或创造更多选择。

参与者不应感到被逼迫或胁迫而自动延长MAST。无论如何，参与者都应从MAST中习得技能，使其能在没有三人组支持的情况下，处理任何未披露的负面生成信念。

5；"我又开始焦虑了，说明还没到离开的时候"

当MAST临近尾声，部分参与者难免对独自面对未来感到不安，担心MAST结束后自己会"崩溃"。这种恐惧会触发症状复发，使他们误以为病情在恶化而非好转。

此时需提醒他们：感受不等于事实（例如 "我感觉MAST结束后会复发，但这并不意味着真的会复发"）；这种体验很常见；尽管存在当下焦虑，他们作为自己的支持者已取得了显著进步；MAST之后发生的事尚未"注定"。

尽管参与者通常感激获得的支持（"没有大家的帮助我做不到"），支持者需抵制过分居功的冲动（"哎，你这么一说..."），将主要功劳归于每位参与者自身。

需强调的是：我们在MAST期间共同探讨彼此的问题，而每个人每天24小时、每周7天都在应对自身困境，而MAST的会期仅为8、10或12小时。

[image]

保持MAST训练成果

实现目标的过程与维持目标的过程截然不同（例如：健身后保持体形；减肥后维持体重）。部分参与者可能认为，一旦MAST结束，他们的收获就会"神奇地"保持不变而无需额外努力；认为辛苦付出后理应获得长期休息；或者认为MAST只是一个独立的、危机驱动的阶段，如今终于可以欣慰地将其抛诸脑后了。如果未能持续践行在**MAST**中艰难习得的技能，我们极易重蹈自我挫败的思维和行为的覆辙 —— 因此必须建立维持性思维模式，以降低这种情况发生的概率。

为开启相关讨论，我们应自问："MAST结束后如何延续你的进步？"；或 "十次MAST课程能否提供终身保障，确保我们永不倒退？" 从本质上讲，需要一种个性化定制的维护心态来保持和加强每个参与者的成功。

例如，某参与者的维持原则是"用进废退"，另一人则是"定期检查认知回路"（他从事电工工作）。参与者可参照MAST疗程安排自我疗愈时段，自主设定议程：设计并复盘MAST任务、评估现状、应对当前困境、预判未来挑战。建议记录自我疗愈时段的具体日期。

参与者需警惕可能导致复发的预警信号，并备有预先制定的行动方案（家人、朋友及同伴也可协助识别预警信号）。以下为具体示例：

某参与者在超市排队时感到燥热难耐，产生"冲出去逃离"的冲动以躲避想象中的灾难。但参与者通过治疗中进行的实验，有力地提醒自己恐慌症状无害且不危险："我的恐慌感会像往常一样迅速消退，一切都会好起来，所以保持冷静。"

她还记住了治疗中学到的五分钟法则：如果停止用焦虑念头吓唬自己，恐慌持续时间绝不会超过五分钟。这是医学事实。由于战斗或逃跑反应产生的肾上腺素会在五分钟内代谢完毕，只要不再产生新的焦虑念头引发肾上腺素分泌，恐慌就会终止。（控制思维控制了恐慌；参与者留在队列中，症状逐渐消退。）

某参与者的伴侣指出 "亲爱的，你又开始了" —— 指她反复纠结工作中的失误。过往失误曾导致情绪低落与自我谴责。此刻伴侣的"轻推"促使她重温治疗中的宝贵领悟："错误不可避免，为之懊恼却非必然。" 怀着这份觉知，她记录下如何修正错误并从中汲取经验。

另一位参与者因旧日 "不值得被爱" 和" 被遗弃" 的恐惧复燃，在关系中再度感到"黏人"。为强化"无需依赖爱也能幸福" 的信念，她刻意独处，重新确认了享受独处的“本领”。正如她告诉伴侣的："当黏腻感消失时，我们才能真正享受美好时光。"

维持并强化治疗成效的另一途径是让参与者向他人传授治疗中习得的MAST技能。例如向朋友解释婚姻破裂时应考量所有因素而非自责："我在治疗中学会了审视全局，而非只关注自身责任。" 通过传授他人，参与者能持续深化对这些宝贵解决方法的理解。但需注意避免以"万事通"或解决问题的典范自居，否则可能疏远他人而非鼓励其倾听学习。学员还可将MAST技巧应用于生活中长期回避或新近出现的困境 —— 例如：对霸道的同事据理力争，或坚决要求新邻居调低震耳音乐。

自我疗愈

> “所有疗法，本质上都是自我疗法。”—— 心理学家卡尔·罗杰斯

三人组会话作为评估改变的场域存在局限，因其脱离了叙述者的日常体验。当与三人组会话并行时，自我疗法能让个体在真实情境中检验并修正其不适应的思维模式与信念体系。

自我疗法工具能帮助个体以日益增长的自信与能力运用**MAST**疗法所习得的技能。若缺乏此环节，参与者往往陷入"情感积压"（等待下次疗程"倾诉一切"），而非及时处理突发困境。因此，从首次会谈起，就应该鼓励MAST参与者立即开展自我治疗任务，而非等到熟悉MAST模式后才实施。

应将自我治疗视为治疗不可或缺的核心环节，而非可选的辅助程序。自我疗法之所以成为MAST的核心要素，在于它不仅能促成长期改变，更能帮助个体持续改善心理健康，摆脱对三人组模式的依赖，避免陷入向支持者寻求问题答案的危险境地。

毋庸置疑，对于严重或根深蒂固的心理健康问题，三人组疗法这种短时干预手段不足以实现可持续的改变。三人组是达成目标的手段，而终极目标正是自我疗愈。

[image]

自我疗愈是一套技术体系，使个体能够运用在三人组中习得的工具以实现自我改变。

通过自我疗愈，参与者能发展成为解决自身问题的自主支持者，不仅能降低全面复发（原有问题再度显现）的风险，更能避免陷入依赖支持者解决问题的困境。

虽然模型不变，但独自实践时的操作技巧显然有所不同。当个人每周固定安排时间进行练习时，自我疗法效果最佳。每周约四十五分钟至一小时的时间，足以有效运用技巧并进行反思。这种正式的自我疗法还应辅以即时实践 ——当 个体遭遇负面情绪或行为困扰时，可随时进行补充性疗愈。

在自我治疗中，个体同时扮演三人组模式中的两个主要角色：叙述者与支持者。所有技术都要求个体在这些角色间切换以促成改变。不同阶段采用不同技术：例如，揭示生成信念的技术与创造替代信念的技术不同，而后者又不同于用新替代信念取代旧生成信念的技术。

创建情境图式

创建情境图式是理解事件中认知元素并识别破坏性认知扭曲的有效方法。个体只需简要叙述导致不良情绪或行为的情境（即扮演叙述者角色），随后尝试识别刺激源、认知扭曲、影响刺激理解的信念，最终剖析这些信念/扭曲引发的行为与情绪。这种简单而灵活的技术能将叙述性经历分解为各个部分，进而运用三人组疗法中学习的各种工具进行分析 —— 例如数据收集或反证工具。运用情境图式是自我疗愈的良好起点，且实施起来相对容易。

"又将如何" 只是揭示生成信念的众多技巧之一。当个体完成多次图式分析后，可能会发现相似或反复出现的信念。这些信念很少是真正的生成信念，更可能是图式中呈现的叙事性合理化解释，或是对情绪/行为反应"成因"的意识层面理解。个体选取其中一个反复出现的中间信念，聚焦最坏结果反复追问 "又将如何"。通常需要多次深入追问才能触及生成信念。例如某人发现社交场合引发焦虑（情绪），并因此停止交谈（行为），源于自我评判的感受。此时需记录对"又将如何"的回答。可能得到"人们会觉得我很愚蠢"的回答。如果继续追问，可能得到"人们不愿和愚蠢的人相处"。第三次追问时，答案可能是"如果他们认为我愚蠢就会离开我，我将陷入孤独"。由此可见，这个回答更直指核心—— "人们会评判我"，将当事人推向了生成信念的深处。这如同剥洋葱般，每层剥离都显露出更深层的信念本质。

建立有效替代信念的有效技巧是运用三人组练习中的建模工具。选择一位你认为能以理想方式应对特定情境（刺激）的人。详细记录你认为对方会展现的行为与情绪。有时甚至可直接询问对方在该情境中的想法感受。接着尝试理解：要使自身信念与之相符，原生信念的哪些部分需要改变？先写下原生信念，再通过调整措辞使其与期望的行为/情绪保持一致。尽量减少修改次数（这将大大降低实践难度）。对每次修改进行难度评估（此方法应已在三人组训练中掌握），这能让你预判替代信念的实施难度。将修改后的信念记录在便于随时查阅的地方。

可视化和日记

可视化与日记记录是成功用替代信念取代旧有生成信念的关键技巧。

可视化即构想情境，并写下你期望在持有新替代信念时产生的情绪与行为。可从回顾过往事件入手，运用新的替代生成信念推测结果会如何不同。这能强化替代信念，无需等待自然事件发生。

日记记录能精确追踪旧生成信念与替代生成信念的运用频率。

虽然需要时间积累，但随着旧信念影响力的减弱，替代信念将逐渐占据主导地位。日记通过强化意识化过程，为信念替换提供强有力的支持。

针对不同议题可采用多种技术，这些议题可能处于治疗过程的不同阶段。无需每次只处理单一问题。显然，若同时处理多个议题，每次自我治疗的时长可能相应延长。达成相同目标还存在诸多其他技术手段。本章仅展示了每个步骤中的一种技术，但每个阶段都存在多种不同类型。读者可在认知心理学、认知行为疗法（CBT）、辩证行为疗法（DBT）、理性情绪疗法（RET）及心理学相关书籍网站中找到更多案例。此环节是疗程的关键环节，若想通过**MAST**获得持久成效则不可省略。此外，本手册还收录了简·亚当斯成员们通过个人或团体实践探索的其他心理治疗学派工具与理念。

自我疗愈的持续支持

在完成MAST疗程后，人们可能难以持续进行有效的自我疗法。这种情况相当普遍，在某种程度上也是意料之中的。生活的挑战和繁忙的日程往往会轻易击垮最初的决心，因此，制定切实可行的计划来维持自我疗法并将其融入日常生活至关重要。对某些人而言，寻求外部支持是实现自我疗法持续性的最佳途径。

[image]

自我疗法的支持形式多样。首先探讨可自主建立的支持体系，继而说明寻求外部支持的途径。显然，在改变产生信念的过程中，结合运用这些方法能最大化支持效果。

对人类思维运作规律产生兴趣，是支持具体自我疗法技巧的良方。这通过将心理学融入生活更多层面来实现，从而更易觉察自我疗法中运用的技巧。如果仅在进行自我疗法时才关注自身心理，很容易将其搁置或彻底遗忘。从某种意义上说，你与它疏远了，是因为它偏离了你的日常生活。通过书籍、博客、媒体文章等阅读一般心理学将有助于保持心智处于心理学框架中。心理学内容不必与认知心理学或你正在使用的技术直接相关，它就可以对你正在做的工作起到补充作用。

制定标准化的自我疗愈时间表是强化疗效的绝佳方式。每周安排两三次、每次十五到二十分钟实践MAST课程所学的自我疗法技巧，效果显著且能巩固进展。有人发现睡前练习比其他时段更有效，但无论何时进行都能为你的工作提供宝贵支持。设置手机闹钟或记录在计划本上，都是轻松安排这类反思与实践的便捷方式。

记录每周甚至每月自我疗愈的效果，是极佳且简便的自我支持方式。为达到最佳效果，撰写新记录前建议重读一两篇旧日笔记，这能帮助你进入反思的正确心境。书写形式通常无关紧要：可叙事可罗列数据点，可打字可手写甚至录音，可详述可概括，可用文字或图像，可主观可客观。这种支持机制既能激励你持续自我提升，又能提供重要反馈，让你清晰看到进步轨迹。它还能帮助你辨别哪些方法对自身成长更有效。

冥想与正念技巧可作为自我疗愈的辅助手段。众多冥想技法中，许多无需经年累月的训练即可实践。能静心聚神的冥想是支持自我疗愈的宝贵资源。正念则是治疗师开发的新型实践体系，旨在帮助个体扎根当下，专注于自身当下的思绪与感受。虽然它与冥想不同，但为自我疗愈提供了类似的支持，且任何人都能轻松学习运用。

进行自我疗愈时所处的环境，可能对疗效产生负面或积极的影响。对许多人而言，拥有一个安全、舒适且井然有序的空间进行自我疗愈至关重要，这能直接提升疗效。如果你居住的环境缺乏这些特质，不妨另觅一处具备这些条件的场所进行自我疗愈。

[image]

自我疗愈不宜在分心、疲惫或过度刺激的状态下进行。

进行疗愈时应远离手机、网络、音乐、邮件等生活干扰源。

疲惫状态下的疗愈往往适得其反 —— 疲惫的大脑难以吸收新信息，也难以进行深度自我审视。药物与酒精同样会阻碍自我疗愈进程，并引发多种神经障碍。

最佳状态是在充分休息、远离电子设备且保持清醒时进行自我疗愈。

有时你可能需要额外的外部支持来维持自我疗愈进程。外部支持可分为两种形式：非正式与正式。当动力减弱或因缺乏进展而陷入停滞时，这两种支持都能作为辅助手段，助你暂时重回自我疗愈的正轨。外部支持应在尝试上述方法之后感觉仍不足以支撑时启用。归根结底，MAST的核心在于自我效能，外部支持应尽可能节制使用。

非正式外部支持包括战友、朋友和家人。对某些人而言，通过分享自我疗愈过程更易坚持疗愈工作。这通常涉及洞见交流、困境分享与愿望倾诉，也包含获取他人对进展的客观反馈。为确保效果，对方需明确了解你的改变目标及具体方法。要使此类支持有效，必须阐明旧有生成信念、替代性生成信念及所用技巧。每次交流应控制在半小时内，否则易令对方不堪重负。且应隔次会面（或更少频率）进行，否则可能改变关系性质。

不言而喻，此类交流仅限于已经建立深度信任的人际关系。与MAST疗程不同，非正式支持者往往倾向于提供建议。你可明确告知对方：你并非寻求建议，只是希望有人倾听你的探索过程。如果感觉非正式支持无法满足需求，再考虑寻求正式外部支持。

正式外部支持包括治疗师、咨询师、生活教练等专业人士。这种关系被定义为单向且结构化的支持（不同于非正式支持），可能涉及服务付费。当其他支持方式都失效时，或当你需要客观外部视角时，正式外部支持尤为有效。此类支持既可避免损害人际关系，又能在长期需求中持续提供帮助。如果你当前缺乏足够安全的或信任的人际关系网络，正式外部支持同样是有效选择。

充分准备有助于确保外部正式支持的有效性。首先应明确说明期望通

过外部支持获得什么。尽可能具体明确，包括：计划接受支持的时间长度；最适合您的支持方式；自我疗愈中遇到的困难领域（如动力维持、反思能力等）；如何判断已获得所需支持；以及如何识别支持关系失效的迹象。您应能清晰直接地回答所有这些问题。也可补充其他需求，如支持者的性别、费用、地点等。完成书面规划后即可开始寻找支持者。当你与支持者见面（面对面或电话沟通）时，应向对方提出问题并告知你准备好的期望。这将使双方建立清晰的预期。建议每四次左右会谈后重新评估这些期望。如果正式支持者不愿回答问题或无法达成共识，请另寻他人。

为充分利用外部支持，请务必遵守预约时间并提前准备：明确讨论内容，必要时可撰写笔记。无需刻意取悦治疗师 —— 您参与治疗的目的是推进自我疗愈进程。若感觉疗效不佳，应及时寻求新的外部支持。

[image]

第八章：互助与工具运用

我们期待你不仅将这些工具用于自身，更要施以援手帮助他人。互助是整个过程的重要环节。通过帮助他人，许多人发现自身能力得到提升，某种意义上也是在助己。在人生旅途中，我们总会遇到需要心灵澄澈的亲友，此时这些工具便能派上用场。无需开展正式的MAST疗程即可运用这些工具助人。

请谨记：透明度是过程的一个关键方面，非正式地向朋友解释你使用的任何工具将对他们更有帮助。你可以这样开始："我也有一个类似的问题，当我经历 MAST 时，我学到了认知扭曲，我认为你可能正在经历这个。"你可以问类似于 **MAST** 会话中支持者的问题，并指出何时出现了自发时刻或认知扭曲。如果他们似乎有兴趣，你可以建议他们查看简·亚当斯网站或将这本书送给他们。

您亦可在社区发起互助疗愈小组。全部所需仅是本书和一个安静的场所，可从共读全书并开展疗愈环节开始 —— 这正是我们的起点！互助自助疗法不存在专家 —— 它是一套开源且持续演进的技术体系，旨在帮助人们实现人生转变。

结语

对简·亚当斯集体而言，互助自助疗法是一场伟大的探索之旅。过去数年间，我们欣喜并见证了众多同志实现生命蜕变。而实践MAST、在社区开展疗愈活动及撰写本书的过程，同样深刻改变了我们自身。**MAST**并非终极解方，而是激进社群认真对待心理健康的广阔尝试之一环。我们坚信：唯有成为有效的人类，方能成为有效的行动者。在这个功能失调且充满压迫的社会里，无人能毫发无损地走出来。我们目睹太多同志因本可解决的精神健康问题而离开社区。我们需要每个人！

愿此书能为其他更多激进社区提供帮助。期待人们持续完善这个过程，使其成为专属的实践。如果您曾使用过它，我们非常期待聆听您的实践经验。

[image]
[image]

互助、创伤和复原力：心理安全 S08E02

[image] 关键词	互助 共生 内讧 反叛 孤独孤立 心理安全 抓特务 抵抗 整体安全 社区
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月3日
[image] **Description**	心理安全

事实上，如果没有创伤，几乎没有什么能阻止反抗者瓦解权力结构。创伤是维系暴政体系的廉价而高效的工具，无论其形态是家庭暴政还是国家暴政，没有区别。

真正发挥效力的并非创伤本身（往往并非如此），而是其衍生的恐惧、羞耻和致残性创伤后遗症 —— 这正是从政府高官到普通家庭餐桌，各种暴君们无处不在的首选手段。

- Table of Contents

  引言
  简·亚当斯集体
  创伤
  创伤与创伤后应激障碍
  定义
  简史
  创伤与PTSD：症状与影响
  安全与创伤
  安顿技巧
  PTSC：创伤后应激社区
  复原力

复原力导论
复原力因素
个体层面
社群层面
复原力：反抗者的武器
应对压力的规划：案例研究
消除羞耻感
打破孤立
与抗争的联结
建立复原力
构建个人复原力
集体复原力
引导性问题
群体问题
个人问题
延伸阅读

[image]

引言

任何反抗权威的行动 —— 无论以何种形式发生 —— 都必然伴随着深陷绝望处境的艰辛。

无数人为我们心目中向往的解放事业献出了生命，见证者亦背负伤痕。

关怀与抗争同等重要，二者缺一不可，往往紧密交织。

对于我们这些与权威对抗的人而言，注定要承受殖民者和法西斯分子施加的暴力后果 —— 这种暴力既是日常的，也是先发制人的，更是直接报复我们追求互助共生的世界的行动。

对我们而言，这些后果的残酷性常以短暂爆发式呈现 —— 我等多围绕这类爆发状况制定防御策略 —— 但必需知道，更隐蔽的伤害是长

期被侵蚀的集体情感福祉。

这片战场我们再熟悉不过了：幻灭、绝望、倦怠、孤立。正是在这片战场上，应对策略匮乏，关怀之责分配极不均衡。

[image]

本集内容旨在为认同互助集体关怀之价值能力的人们提供资源，

助力拓展集体应对创伤的知识和实践。

请记得，任何文本都存在局限性 —— 我们最珍贵的资源始终是彼此及相互扶持的关系。

作者将情感韧性视为需集体构建与实践的对象 —— 它需要盘点、需要休憩，更应成为应对创伤时调用的指引力量和原则。我们的概念体系植根于对创伤、创伤后应激障碍（PTSD）和创伤后应激连续体（PTSC）及其特征的认知，相关阐述详见后续章节。

我们认为，将集体创伤认知植根于其独特的概念与意识形态历史具有重要意义；我们的核心宗旨在于提供替代方案 —— 摒弃那些广为流传的新自由主义“自我关怀”观念。这些观念不仅强化了资本与国家权力的霸权，更使我们陷入无力感与孤立状态。我们致力于传播韧性作为一种方法论，以对抗各种压迫性势力用以分裂和削弱我们的创伤武器化手段，从而建立起我们长期反抗这些力量的能力。

简·亚当斯集体

简·亚当斯集体在纽约市历经至少五年的演变历程。我们的成员包括社会工作者、心理治疗师、以及其他反抗精神健康领域等级制度话语体系的抗争者。本集体的成立源于激进派空间中情感支持的需求，并由此开启了一场名为"互助自助疗法"的替代性关怀实践实验，这项实验至今仍在持续推进。

“主流”的自我关怀叙事往往将情感需求商品化而非满足需求。在“医疗化”的心理治疗领域，个体被迫陷入客户-提供者的权力关系中，那些本可以自主提升自我的工具和知识被刻意隔绝难以获取。

治疗师佯装洞悉患者情绪根源，同时垄断其掌握的知识，以此确立自身话语的权威性，在来访者心目中强行树立权威形象。

我们发现，通过集体协作改变不良情绪与行为模式，以缓解权势压迫带来的痛苦，是构建反权力社群的集体实践和战略组成部分。我们视共同满足需求为强化社群的契机 —— 不仅通过互助解决当下或长期的困扰，更通过在亲密与脆弱中建立信任，宣告心中理想的新社会不应让情感坦诚蒙羞。

[image]

创伤

创伤与创伤后应激障碍

定义

创伤可定义为具有重大心理影响的事件。它破坏个体的自我认知、世界观或对未来的展望，进而影响其对人生意义与目标的感知。可以说在创伤发生的瞬间，幸存者会因压倒性的力量而陷入无助状态。

急性创伤通常与单一事件相关，而慢性创伤则指持续性、长期性且反复发生的创伤事件。心理创伤可表现为强烈的恐惧感、无助感、失控感、及灭绝威胁感。创伤体验具有个体独特性，且难以量化，但为应对并尝试走出阴影，对其进行命名具有重要意义。

简史

创伤研究的历史可追溯至对癔症、战斗神经官能症及性暴力的研究。当时，癔症被用于将女性病理化，其根源在于性创伤。创伤事件引发难以承受的情感反应，导致意识状态改变 —— 当时称为癔症，如今则称为解离。弗洛伊德等学者终止了对癔症根源的研究，因继续探究将迫使他们直面人性中某些残酷的真相 —— 例如施加严重虐待的能力。于是将虐待记忆归咎于癔症幻想便成了更便捷的解脱方式。女性因遭受虐待而背负污名，大量虐待事件在恐惧与羞耻的压制下隐匿于公众视野之外，这种沉默反而助长了更深层的剥削。

关于创伤性障碍的早期知识体系，很大程度上源于对一战后经历战斗的男性的研究。治疗最初被称为"谈话疗法"。PTSD的概念最终诞生于对退伍军人的研究，其目标是“修复”他们以便重返战场。当时某些研究甚至对患者进行道德评判，将人视为手段而非目的。

1970年代女性解放运动期间，意识觉醒团体开始涌现。意识觉醒团体类似心理治疗小组，但其宗旨在于推动社会变革而非个体改变。女权运动重新定义强奸为暴力犯罪而非性行为，并创立新术语以阐释性侵的影响。1971年首次举行公开谴责强奸的集会，但强奸改革立法直至1970年代中期才得以实施。随着创伤事件应对机制的研究深入及女性议题获得重视，研究发现不同群体对创伤的反应具有普遍性。在退伍军人推动创伤后应激障碍（PTSD）获得医学认可后，人们逐渐意识到家庭暴力与性暴力幸存者呈现出与战争幸存者相似的症状。该诊断标准直至1980年才被正式纳入《精神疾病诊断与统计手册》。

创伤与PTSD：症状与影响

创伤后应激障碍（PTSD）的症状可能扰乱患者的生活，使其难以继续日常活动。症状通常在创伤事件发生后不久出现，但也可能延迟数月甚至数年才显现。这些症状还可能在多年间反复出现。

多数经历创伤事件的人初期会出现某些症状，但不会发展为PTSD。若症状持续超过4周，引发严重痛苦或影响工作家庭生活，则可能属于PTSD范畴。

PTSD症状主要分为四类：

1. 创伤事件的侵入性重现。

创伤记忆可能随时涌现，伴随事件发生时的情绪体验，常表现为噩梦和闪回。

1. 回避行为。

可能刻意回避触发创伤记忆的情境或人物，甚至拒绝谈论或思考该事件。

1. 信念与情感的改变。

创伤经历改变了对自我及他人的认知方式，具体表现包括：

- 对他人缺乏积极的情感或爱意，可能回避人际关系。
- 可能遗忘创伤事件的部分细节，或无法描述这些内容。
- 可能认为世界充满危险，无人值得信任。

1. 过度警觉。

可能表现为神经紧张、时刻戒备着危险。例如突然暴怒易怒、睡眠障碍、注意力涣散或易受惊吓。

暴力的不可预测性会引发过度警觉。创伤瞬间仿佛时间凝滞。许多创伤记忆缺乏语言叙述和情境背景，而是以鲜活的感官体验和画面的形式编码存储。

初期以创伤事件的侵入性重现为主（噩梦、闪回），幸存者持续处于高度焦躁状态，时刻警惕新威胁的出现。侵入性症状在创伤事件发生后的最初几天或几周最为突出，三至六个月内会有所缓解，随后随时

间推移逐渐减弱。尽管特定创伤症状看似随时间消退，但原始创伤的提示物仍可能（甚至在事件发生多年后）重新唤起这些症状。创伤事件似乎会重塑人类神经系统。创伤的重复经历会加剧所有PTSD症状。心身症状源于自主神经系统的持续激活。

当幸存者沦为囚徒、无法逃脱且受到施暴者的控制时（如虐待性家庭、性剥削、监禁环境），便会遭遇重复性创伤。施暴者通过心理控制手段灌输恐惧和无助感，摧毁幸存者自主意识及与他人相关的自我感。成年期反复创伤会侵蚀已形成的人格结构，而童年期反复创伤则塑造并扭曲人格。其造成的损害可能干扰儿童建立安全依恋关系、发展认知能力、情绪调节、行为控制、自我概念及生理成熟，并增加解离倾向。

同时显著提升自残与自杀行为的发生概率。

所经历的虐待程度与解离倾向存在相关性。幸存者可能经历麻木或恍惚状态作为解离形式，这在急性创伤期间能降低其对疼痛的感知。当事人自己无法控制何时进入这些改变状态，这些状态将痛苦记忆与日常意识隔离。这不同于主动压抑创伤相关记忆以抵御强烈情绪反应的行为。

在持续面临真实危险的环境中，此类机制具有生存意义，但脱离该环境后便会演变成适应不良。

以下是一些可识别的创伤性情境：

- 替代性或继发性创伤
- 儿童虐待
- 性暴力
- 家庭暴力

- 自然灾害
- 战争
- 社会/生活环境相关创伤（如社会压力）
- 系统性或制度性暴力与虐待
- 代际创伤
- 医疗相关创伤
- 丧失

创伤事件在基本身体完整性层面侵犯了个体的自主权。它们干扰了自我认知，经常导致幸存者感到与他人及社群相隔绝。创伤者不仅在思想和梦境中重温创伤时刻，更会通过行为再现创伤场景。这种再现可能是试图重历并掌控创伤事件带来的压倒性感受。

[image]

无助感构成创伤的核心伤害，而修复过程需要重建效能感与掌控力。据称，这种再现行为正是个体修复创伤所需的情感体验。

幸存者易陷入自责的情绪。这种内疚可理解为试图从创伤事件中汲取有益教训，以重获掌控感。想象自己“本可以做得更好”，或许比直面彻底无助的现实更易承受。当幸存者目睹他人受苦或死亡时，这种自责感尤为强烈。

由于侵入性症状与麻木症状均无法整合创伤事件，这两种极端状态的交替或许可理解为寻求平衡的尝试。但平衡恰恰是创伤者所缺失的。创伤者发现自己被困在遗忘与创伤重现的两极之间，在汹涌的强烈感受与情感枯竭的荒漠之间，在易怒冲动的行为与完全抑制行动的状态之间。这种周期性转换引发的不稳定性，进一步加剧了创伤者对不可

预测性和无助感的体验。因此创伤的辩证关系具有自我延续的潜在特性。

遭受创伤的个体，尤其是童年及青少年时期受创者，更易出现以下风险：

1. 社会行为问题，包括但不限于：人际关系障碍、危险性行为及攻击性行为。

1. 终生心理健康受损，包括但不限于：创伤后应激障碍、抑郁症、物质滥用及自杀倾向。

1. 童年逆境经历还与多种心理障碍的发生密切相关：

- 认知与学业问题，包括但不限于：智商及阅读能力低下、语言认知发育迟缓、学业表现不佳。

- 神经心理改变，涉及调节情绪、情感控制、判断力、解决问题的大脑区域，以及应激反应系统。

- 持续数十年的身体健康损害，如癌症、心脏病、肝病、肺病、自身免疫性疾病和肥胖风险增加。

- 更高比例的精神卫生及医疗服务使用率。

- 失业率、贫困率及医疗补助使用率上升。

- 童年死亡或早逝。

此外，拥有4种或4种以上不良童年经历的成年人，患以下四类疾病中每一种的几率要高出**7.3**倍：：

- 情绪障碍
- 焦虑障碍
- 冲动控制障碍
- 物质滥用障碍

女性比男性更易患创伤后应激障碍（PTSD），且更易发展为慢性PTSD。研究发现，在退伍军人中，抵御极度恐惧的最强保护因素是士兵与战友之间的亲密程度。人际关系、情感联结以及对生命意义的感知，对缓解PTSD至关重要。必须正视创伤幸存者的心理反应，这有助于重建控制感，并建立更牢固、更健康的人际关系。

[image]

安全与创伤

如果创伤源于感知到自身或者所关切的其他生命体存在生存威胁，那么治愈创伤的关键步骤便是确保自身及他人免受生存威胁的安全感。

鉴于现代生活的复杂性，这些威胁往往具有多重维度且错综复杂。阻碍安全感的因素包括但不限于：食物匮乏、居住环境不安全或无家可归、社会支持不足、情感/身体虐待、直接暴力侵害、以及自毁型行为模式。

相较于"安全"，"资源充足"或许更能准确描述这种状态 —— 即个体拥有多少必要资源，或获取资源的便利程度。即使最初的创伤事件或情境仅涉及单一威胁，其他领域的威胁仍可能使已受创者再度受创，因为这些威胁会影响个体对心理安全的感知 —— 而这种感知破裂正是创伤的初始根源。

对某些人而言，规划如何为自己和他人提供安全保障，并证明自身执行计划的能力，是创伤康复的重要环节。

[image]

作为试图疗愈自身或身边同志创伤的无政府主义者，建立并维系团结纽带尤为重要 —— 毕竟社会支持与物质资源对安全感至关重要。

更何况，我们提供安全保障的努力可能面临政治生活的挑战：监禁、警察暴力及国家其他镇压手段都构成必须正视的现实威胁。

制定一项或多项安全计划，并确保有值得信赖的同志执行，可成为应对这些障碍的有效工具。尽管我们的行动主义及与国家的对抗关系可能构成安全隐患，但基于无政府主义同志及其他社群真实团结建立的非资本主义联结，在此领域反而能成为优势。

互助与团结网络 通过共享资源并扩大资源获取渠道，能够满足安全需求。

安全与创伤的关系揭示了一个重要启示：根据个人生活境遇（包括社会支持、经济保障、食物、住所及自我防卫能力的可获得性），最有效的创伤康复策略或许是完全避免探索创伤记忆。防止二次创伤本身就是值得追求的目标，在特定情境下更是个人力所能及的最佳选择。审慎等待直至确认安全后再探索创伤记忆，这并不可耻 —— 它是疗愈过程的必要环节。创伤治疗师朱迪思·赫尔曼如是说："建立安全感这项任务优先于其他所有工作，因为如果安全感未得到充分保障，任何治疗工作都难以成功。在达到合理安全程度之前，其他治疗工作都不应尝试。"（《创伤与康复》第八章"安全"）

对于那些正等待探索创伤记忆并致力于建立安全感的人而言，其创伤疗愈过程在旁观者眼中，可能与非创伤性心理健康问题的自我关怀工作相似。此时的核心差异在于意图。当安全感获得可靠保障后，便可着手发掘并重新诠释创伤记忆，此时再次受创的风险已得到有效控制。由于创伤疗愈并非线性过程，且构筑安全感的生活环境具有流动性与变迁性，因此持续性地不定期重新审视安全问题，是关照自我与他人的有效方式。

安顿技巧

安顿：指透过感官接触自然来获得稳定的一种练习。

当我们陷入痛苦时，安顿技巧（也称“定心”或“健康抽离”）能发挥重要作用。其原理在于将注意力从内在的自我转向外部世界，可在任何情绪痛苦时刻实施。这些技巧虽简单易行，但需频繁练习方能发挥最大效用。丽莎 M·纳瓦吉蒂斯在《寻求安全：创伤后应激障碍与物质滥用治疗手册》中提出三种安顿方式：心理安顿、身体安顿与舒缓安顿。

1. 心理安顿包括运用所有感官详细描述环境，或细致描绘日常活动。想象时可借助画面：例如想象自己在切换电视频道寻找更精彩的节目。想象在自己与痛苦之间设置一道缓冲屏障。

1. 身体安顿包括专注于呼吸，感知每次吸气与呼气；觉察身体状态；触摸周围物品并感受其质地、色彩、材质、重量与温度。

1. 舒缓式安顿法包括：重复应对宣言（比如 "我能处理好，这种感觉会过去的"）；回忆安全场所并专注于其色彩、声响、物品与质感；想象珍视之人与期待之事。

如安顿法效果不佳，请尝试增加练习频率和时长（20～30分钟），或在条件允许时寻求他人协助。

[image]

PTSC：创伤后应激社区

创伤不仅可能对个人生活造成持久伤害，更可能摧毁政治组织、社区及社会运动。创伤是抵抗过程中不可避免的组成部分，社区在开展工作时应预见到会遭遇各种形式的创伤。正如并非所有经历创伤的个体都会发展出致残性慢性症状，并非所有政治社群都会因创伤而遭受（长期）损害。PTSD（创伤后应激障碍）是描述个体创伤常见负面症状的术语；我们在此将PTSC用于社群的类似情境。慢性创伤对个体造成的负面影响及生活后果已被充分研究阐述，但群体层面却鲜少受

到关注。本节将阐明慢性创伤对群体产生的常见负面效应。

[image]

过度警觉是PTSD最常见的症状之一（如前文所述），也是社区遭受创伤影响的典型警示信号。在群体环境中，过度警觉表现为持续搜寻威胁。

常见形式是识别并标记"不安全"的个体或群体，告密者（线人）标签化与搜寻内奸/停不下来的“抓特务”便是典型例证。

较不显着的是，当患有PTSC的群体对陌生人日益警惕时，新成员招募量会减少。这种症状也可能建立起复杂的担保机制，同样会降低参与度，并凸显参与者之间彼此的可疑性质。

这些行为实际上并没有增强群体安全感，

因此当其源于创伤引发的过度警觉时，便构成了病理症状。

倦怠是**PTSC**的另一常见症状。倦怠并非必然源于PTSC，个体退出团体可能出于多种与创伤无关的原因。然而，未能建立创伤处理机制的团体中，参与者的倦怠程度往往显著升高。压力是导致倦怠的强大驱动力，团体中未解决的创伤会持续向参与者传递压力。

长期创伤使得无论是个体还是群体都难以安全地应对世界；故这种不安全感会导致群体更大的孤立。

[image]

患有PTSC的群体往往回避与立场相近的其他群体建立联盟或伙伴关系（尤其当“对方未经历相同创伤”时）。

这类群体通过缩小认知世界、退守熟悉的保护壳来寻求安全感，通常拒绝参与新的运动、项目或联盟。

这可能导致群体产生地下化运作或秘密行动的迫切需求，从而与盟友及支持网络割裂。

内斗是群体中慢性未愈创伤的典型特征。创伤往往破坏了建立多元群体工作联盟所需的基本信任感与稳定性。当信任、理解和稳定性遭到摧毁，内斗与纷争便不可避免。

绝望感 - 毁灭型虚无主义（如大洪水论） - 也是**PTSD**和**PTSC**的典型症状。慢性创伤通过持续重复和剥夺自主权，极大削弱了希望感，使我们丧失对自身行动能积极影响预期结果的信念。

抵抗团体本就难以维持行动动力，而这种症状会严重消耗持续开展艰苦政治工作的能量乃至意愿。

以上这些虽非PTSC的全部症状，却是最常见的类型。它们如同PTSD的个体症状般具有强化效应：内斗会加剧精疲力竭，高度警觉则会导致政治孤立，如此循环往复。

镇压当局使用的“平暴”手册数十年来早已洞悉：只要制造创伤性社区，便能做到在不正面对抗的情况下直接瓦解其战斗力。PTSC症状的破坏力极强，能在极短时间内摧毁多年积累的成果与诸多胜利。

虽然我们往往无法阻止敌人对运动造成创伤，但可以采取措施降低PTSC摧毁社区的可能性。

[image]

复原力

复原力导论

复原力是一种心理概念，描述了一系列使个体能够经历创伤而不致患

上创伤后应激障碍（PTSD）的特质集合。

当前心理学家正通过研究经历创伤后出现PTSD与未出现PTSD的群体，并追溯性地考察两类人群的个体及社群特征，试图更清晰地勾勒复原力的图景。尽管这份可能构成统一"复原力"的特质清单中，许多特质难以刻意培养，但我们相信其价值在于提醒我们：作为个体、社区、朋友群体和家庭，我们早已具备其中部分或多数特质。在创伤事件后以创造性且动态的方式主动激活这些特质，有助于抵御**PTSD**的长期影响。

复原力因素

个体层面

- 意义构建
- 抽离、和概念化问题的能力
- 自我效能感与决心
- 自主性
- 坚韧性：承诺、掌控、和挑战
- 自尊和自信
- 利他主义或亲社会行为
- 运用成熟的自我防御机制
- 积极应对而非回避应对方式

- 以问题为中心的应对而非情绪化的应对
- 接纳自身与他人的恐惧
- 缺失或低水平的内疚、羞耻、尴尬
- 幽默感
- 对暴力采取主动应对
- 正念
- 道德指南针或内在信念体系
- 心理准备度

社群层面

- 感知到的社会支持的可得性
- 实际获得的社会支持
- 主动寻求社会支持
- 向重要的身边人披露创伤经历
- 群体认同感和将自我视为积极幸存者的观念
- 与重要社群（朋友及幸存同伴）建立联结、情感纽带、及社交

复原力：反抗者的武器

无论反抗者采用和平主义还是更激进的抵抗手段，都可能直接或间接遭遇创伤。制造创伤体验是任何权力结构最喜爱的必备武器，权力结构越不公正，就越依赖创伤来实施社会控制。

事实上，如果没有创伤，几乎没有什么能阻止反抗者瓦解权力结构。创伤是维系暴政体系的廉价而高效的工具，无论其形态是家庭暴政还是国家暴政，没有区别。真正发挥效力的并非创伤本身（往往并非如此），而是其衍生的恐惧、羞耻和致残性创伤后遗症 —— 这正是从政府高官到普通家庭餐桌，各种暴君们无处不在的首选手段。

个人、群体、组织乃至整个社区都可能因敌对势力策划的创伤事件而被瓦解。这既是恐怖分子的逻辑，也是警察审讯者的逻辑。翻阅基地组织、FBI、日本黑帮或美军野战手册时，令人震惊的不仅是创伤被武器化的赤裸手法，更在于这些组织运用创伤手段的惊人相似性。

就如车轮作为一种工具，因其廉价高效而在各地独立发展。暴虐势力系统性地使用创伤也是如此。反抗者若不主动寻求创伤应对策略，就永远无法抵御这些强大而廉价的压迫武器。

在反抗群体中诱发创伤后障碍尤其阴险，会严重削弱大多数抵抗运动本就有限的组织能力。拿破仑曾阐释使用致残性（通常非致命）霰弹的军事价值："一名阵亡士兵仅导致一条火枪退出战场，而一名负伤士兵可能使两条、三条甚至四条火枪同时失效"。伤员需要敌方投入资源和精力进行救治。精神创伤亦是如此。那些身心残缺者，终将成为压迫者力量与反抗危险性的日常警示。

这一切听起来相当黯淡，但的确存在一种方法能建立复原力，使创伤无法或难以阻挠抵抗运动。

[image]

复原力不仅能削弱创伤的影响，更能让压迫者自食其果。

某种意义上，群体复原力的形成会削弱创伤武器的效力，从而保护那些尚未发展出复原力的个体或群体。当暴君发现创伤手段不再奏效，便会停止肆意施加于他人。

对具有韧性目标施加创伤反而适得其反，反而强化了反抗者或被压迫者的力量，这将彻底改变施暴者对创伤手段的成本效益分析。

此举将极大降低这种武器的使用频率。

要在个体、群体及社区中培育、运用并共享复原力，我们必须先厘清其本质与运作机制。

复原力最常见的两种定义是：从困境中快速恢复的能力；物质或物体恢复原状的弹性特性。显然，反抗者和抵抗运动必然面临敌对势力的打击，而同样显而易见的是：我们应竭力实现快速反弹，遏制创伤的蔓延与持续影响。

运动的韧性越强，就越能吸引那些感受到当前权力结构威胁的局外人。这也会在权力结构内部引发分裂，因为当权者必须权衡施加创伤的效益与引发反弹（即复原力）的代价。如果创伤手段的有效性被证实不足，权力结构内部成员间的控制关系便会显现，从而严重削弱权力体系。

心理复原力的培养常被比作自卫，但其意义远不止于此。运动/社区中成熟的复原力机制，可有效招募那些因现状（无论是否与对抗的权力结构相关）而焦虑恐惧的人群。例如在罗贾瓦，叙利亚北部的库尔德革命力量就吸纳了大量逃离强迫婚姻、家庭暴力及受压迫少数群体成员的加入者。

[image]

除招募外，复原力还能动摇敌对势力根基。

权力结构中的多数参与者（军官、士兵、官僚等）未必真正受益于压迫，却是因焦虑或恐惧而选择站在压迫者一边 ——他 们害怕脱离体系后的后果。

具有复原力的反抗力量能 削弱那些未直接获益者的忠诚度 ，

迫使敌方投入更多资源来招募和维系自身成员。

复原力并非消除创伤事件的护盾，而是让敌人利用创伤手段收效甚微的代价。其机制在于瓦解羞耻、恐惧、内疚、绝望、社会瓦解与孤立等创伤效应 —— 这些正是消解政治行动力的最持久影响。

心理复原力与社群复原力的结合能消除人为创伤的长期效应。创伤会滋生更多的创伤 —— 例如，最初可能需要重型炮弹才能使个体陷入瘫痪、混乱与恐惧；但如果个体缺乏复原力，后续仅需汽车排气管的爆响便能重现相同反应。

复原力则产生反向效应 —— 让敌人制造的每次创伤需要付出更大代价才能达到相同效果。

如果创伤已成为当代压迫的货币，那么复原力便是反抗者的武器。

[image]

应对压力的规划：案例研究

1980年代末至1990年代初，芝加哥的 ACT UP 组织成立了一个名为"可持续行动与关怀委员会"（CSAC）的工作组。该委员会意识到，持续的抗争压力、艾滋病疫情造成的创伤、以及警方暴力，正严重侵蚀着组织活力。他们发现核心组织者不仅面临更严重的倦怠，尽管取得诸多胜利，团体内部冲突却日益加剧。CSAC由心理健康工作者和普通成员组成，负责探索减轻芝加哥 ACT UP 组织内部的压力及创伤后功能障碍的方法。该委员会虽仅存续短暂时间（不足一年），却成功引入创新性创伤缓解技术，不仅在芝加哥分会，更被其他城市的

ACT UP 分会广泛采用。

消除羞耻感

ACT UP 组织倾注大量精力，致力于减轻艾滋病患者、HIV感染者及同性恋群体普遍面临的被污名化与羞耻感。社区支持艾友协会每月举办"自由谈系列"活动，让社区成员能在支持性环境中畅谈压力，免受评判。这对照料艾滋病临终患者的护理人员尤为有益。其设计理念与1970年代女性主义觉醒小组相似 —— 没有预设议程，人人都能在安全环境中畅所欲言。

ACT UP 还邀请各类行动的资深参与者坦诚分享行动经历，涵盖正负面感受。这有助于将人们因警察而产生的恐惧、压力或创伤体验正常化，这些故事有效消解了行动中常见的羞耻感。ACT UP还邀请民权运动、环保运动及反战运动等其他运动的资深人士分享经历与感受。这使人们在高风险街头行动中面对压力情境时产生的各种情绪反应得以正常化。

打破孤立

在手机、互联网和社交媒体尚未普及的年代，ACT UP 各分会就已擅长维系成员间的联系。

CSAC特别设计了多项干预措施，旨在缓解创伤者普遍面临的孤立感。

首创的"肯定派对"活动，会在重大行动后2-3天内按计划举行。活动参与者及支持者均被期待出席派对，筹备过程包含大量策划与宣传工作。

无论行动成败，参与者都会起身讲述行动对个人的意义，借由饮酒、音乐与舞蹈等社交场景，将街头抗争的团结精神延续至行动之后。现场常会向参与者赠送象征感谢的信物（如鲜花、AA式纪念币等）。活

动开始前会宣读社区中因艾滋病逝世者的姓名，随后派对正式启动。此外，CSAC成员会在行动后通过电话联系抗议参与者，有时还会亲自探访。这种关怀让参与者感受到社区的守护力量。

最后，那些遭遇创伤性事件（如警察暴力、被捕或亲友因艾滋病离世）的参与者，会被邀请在下次组织会议上以"资深者"身份发言。这使他们的身份从孤立的受害者转变为受重视的资深者 —— 拥有可与群体分享的经验。

这种机制帮助个体"梳理"情感，从中提炼价值和经验教训进行分享，既可以减轻习得性无助感，又为经历赋予了意义。

与抗争的联结

SCAC极力强调与抗争运动的紧密联系，通过将抗争中的艰辛置于具体情境中，从而减轻参与者的压力。行动前，组织常会向每位参与者发放社区中因艾滋病逝者的姓名与照片，让他们随身携带。如果有人被捕，他们往往会报出那个人的姓名。这个简单举动让人们始终铭记走上街头的初衷。

ACT UP 行动前常举行集会，通过演讲和音乐营造士气，再集体前往抗争现场。这种集体仪式感营造出社区归属感，有效缓解了个体的脆弱感与孤独感。

SCAC还建立了心理健康服务转介网络，为有需求者提供支持。志愿者常陪同初次就诊者前往诊所，在候诊室守候，直至治疗结束。这种朴素的陪伴，正是真诚支持的有力见证。

ACT UP 运用多种技巧来减轻抗争过程中可能遭遇的压力与创伤带来的情感消耗。这些技巧虽经过精心设计，却几乎不需要额外资源或专业技能。它们为构建一种具有复原力的激进文化提供了强大途径，使该文化得以在重重阻碍中持续多年。正如我们需要发展自己的创伤应对机制来建立真正具有复原力的抵抗力量，ACT UP 也借鉴了先前运动和活动家的干预经验。

[image]

建立复原力

建立复原力并非千篇一律的过程，我们每个人都是独特的个体，但无政府主义者在培养承受创伤事件的能力方面比普通人更具优势。复原力建设的协作性与持续性特质，恰好契合我们许多人正在开展的组织工作 —— 前提是我们必须采取有意识且积极主动的方式来培养复原力。

长远来看，如果能建立支持与互助体系来应对创伤余波，处理创伤事件就将更为轻松。但无论拥有何种支持网络，自主构建复原力都至关重要。

构建个人复原力

独自应对创伤事件极其艰难，因此，无论你是否拥有组织伙伴，培养复原力都至关重要。

[image]

身处创伤事件时，人们往往难以保持清醒应对。请在危机降临前，明确自身可调动的社会资源与个人资源。列出危机联络名单，并制定应对方案。

审视即将面临的处境，尝试以战术思维预判。

预知风险、做好准备、学会战术性思考潜在创伤情境，能培养从外部视角审视问题的能力，从而保持必要距离实现有效应对。

创伤风险始终存在于我们的生命中。这是一个需要持续自我修习并影响所处群体的过程。在事件发生前及日常生活中，请提高对自身反应模式与预警信号的觉察力。在压力情境发生前或过程中，能识别身体

感受的变化至关重要。压力时期更应持续自我监测，留意任何预警征兆。

随着时间推移，这种自我认知与持续关注身体感受的能力，将逐步提升你应对各类压力情境的复原力。预知风暴来临，便能从容备战。

[image]

返回 - 相关练习：[image]S01E01-T3 创伤经历如何影响您的认知

练习：[image]S01E05-T2监测自己的压力水平

练习：[image]S01E06-T2 找到弱点建设新的防御能力

当预警信号显现时，采取积极应对策略而非逃避行为至关重要。日常生活中最常运用的应对技巧，正是危机时刻的坚实后盾。

思考应对创伤事件的方法时，请聚焦主动应对技巧而非回避策略。虽然暂时逃离痛苦情境或精神创伤能带来短暂解脱，但如果想处理创伤的长期影响，自我隔离、用物质麻痹自己或回避所有相似情境，都无法让你真正化解负面经历及其后续影响。要建立持久应对心理困扰的能力，更应专注于积极应对技巧 —— 这些技巧能切实改善身心健康，并促进政治与社会参与度。

即便独自面对创伤事件，只要积极参与互助行动，你的应对能力仍会得到提升。持续践行互助不仅改善社会处境，更塑造自我认知与人生目标。当你意识到自己正以积极方式影响世界、建立人际联结、践行有意义的事业时，内心便会滋生力量感与安全感 —— 正是这些特质助我们抵御创伤侵袭。

集体复原力

与你并肩作战、共同闯荡的伙伴们或许早已践行着这些准则，但明确思考行动可能引发的心理影响，并关注团队成员的心理需求，对我们

抵御创伤至关重要。

无论是在具体行动前，还是作为互助支持体系建设的常态化环节，制定应对创伤事件的支援计划都不可或缺。你应当了解战友（以及亲密朋友）的基本情况：当他们难以应对当下困境时会联系谁、哪些经历可能使某些事件对他们更具挑战性、以及哪些方式能帮助他们应对负面情绪。即便这些信息永远无需启用，它们也能在团队中建立安全感与支持感。身边有人懂得在危机时刻如何有效地伸出援手，不仅能提升你未来应对创伤的能力，更能增强集体韧性，加深组织成员间的社会纽带。

制定行动方案并清晰预判风险，同样重要。我们对创伤的长期反应往往与对世界及局势的预期紧密相连。了解行动性质至关重要：举着标语参加游行与加入黑群行动截然不同。在任何行动准备阶段，预判可能发生的状况与风险，都有助于减轻创伤对你的影响。即便不考虑复原力建设，这种分析与战术思考的过程本身，也能帮助群体采取有效行动，提升我们实现政治目标的能力。

这种规划与战略思维是有效组织工作的必要组成部分。在复原力建设方面，以战术思维处理问题有助于提升抽离视角、抽象化思考的能力。我们固然无法掌控所处的环境，但完全能够建立更切合实际的预期，并培养提升效能、减少负面影响的技能。

然而仅针对特定事件的规划远远不够。遭遇创伤事件后，必须通过互助与抗争的直接行动，以协作方式作出回应。当团队成员遭遇创伤时，请主动关怀他们，建立支持机制以满足其需求，并在可能的情况下对施害者采取行动。

[image]

参与直接行动与互助能激发效能感和能力感，从而减轻创伤应对难度。

自我认同、人生目标感，以及被在乎者支持的归属感，对化解创伤至关重要，更是践行我们政治使命的核心要素。

引导性问题

应对潜在创伤与构建复原力的关键，在于培养情感认知与心理准备的实践。孤立与疏离会加剧创伤体验 —— 新自由主义主张的 “自我照护” 是一种刻意加剧孤立疏离的观念，这种观念将关怀定位为个人责任，它非但不治愈伤痛，反而羞辱伤痛者。

倘若我们在行动规划中，像重视身体与战术准备那样纳入情感与心理准备呢？如何更好地关怀自我与彼此？为此，我们为个人、朋友及亲密团队整理了一系列潜在的问题，旨在促进关于应对创伤、构建个体与社群复原力的讨论。

第一组问题聚焦团体规划与决策。这些问题可协助亲密团队或朋友就情感心理准备达成共识，促进对社群关怀的共同理解。

第二组问题聚焦个人经历与需求。这些问题的目标不仅在于提升自我认知，更在于为朋友和同志提供工具，以便在创伤事件发生时支持你，同时也让你掌握支持他人的方法。

创伤反应因人而异，适合你的方式未必适用于他人。提前了解朋友和同志的需求，比在危机时刻仓促猜测更为有效。

创伤事件发生后，当事人往往难以立即回忆或表达自身需求。如果能有一位知情且值得信赖的朋友或同志，将极大助力即时应对与复原力重建。

最后，围绕心理健康与创伤展开开放对话，能有效对抗孤立感与羞耻感 —— 这两者既会加剧创伤效应，又会阻碍康复和复原力的培养。

这些问题仅作为对话起点，无需回答任何令你困扰或不知如何作答的问题，我们强烈鼓励你根据实际情况增删问题。此外，这并非一次性的讨论，而是建立情感认知与心理准备实践的重要环节。这些话题不易启齿，请随时暂停、休息或继续。让我们善待自己，也善待彼此。

群体问题

1. 在行动中，我们每个人能提供哪些支持？（例如：有人出现恐慌发作时我能进行安抚；我能确保团队成员及时补充水分等等）

1. 能否根据成员的过往经历和触发因素，在行动规划中设置不同的职责？

1. 是否需要制定触发点警示信号/安全词，以便在行动中使用？（例如：绿色＝状态良好，黄色＝需关注我，红色＝需要休息/离开）

1. 是否需要携带心理急救包参与行动？急救包应包含哪些物品？（例如：减压玩具、香氛物品、药物、草药、防寒毯等）

1. 是否要在行动后选定日期聚会，共同检视情绪健康状况？无论行动是否顺利都应执行此项？

1. 遭遇创伤事件时如何最佳互助？可规划哪些有益活动？（如集体晚餐、互助小组等）

1. 遭遇创伤事件时，是否需要未在场同志的支援？期望支援采取何种形式？如何传达此需求？

1. 为避免支援者超负荷/倦怠，可建立哪些边界？

1. 如果需心理健康资源，现有哪些可用渠道？

个人问题

1. 紧急情况下您希望联系谁？遇到压力情境时，是否有倾诉对象

能为您提供帮助？在何种情况下您允许他人代为联系您的紧急联系人？是否有您不希望被联系的人？

1. 是否有实物能帮助您缓解压力？（例如减压玩具、石头、毛绒玩具等）

1. 是否有特定场所能缓解你的压力？（如公园、咖啡馆、厨房等）

1. 是否有特定活动能缓解你的压力？（如散步、安静地和朋友坐在一起等等）

1. 是否有任何感官体验能在压力情境中缓解你的情绪？（例如：闻特定气味、触摸冰凉物品等）

1. 是否有需要在压力情境中避免的场所或活动？（例如：被触碰、开放/封闭的空间等等）

1. 是否有希望朋友/团队知晓的过往创伤经历？

1. 是否有希望朋友/团队注意到的触发因素？

1. 对你来说最典型的生理/行为压力反应是什么？（呼吸困难、异常沉默等）

1. 哪些方法曾在创伤情境中帮助过你？（如安顿技巧等等）

1. 哪些方法对即时缓解有效？哪些对长期缓解有效？

1. 哪些迹象表明你状态不佳？（例如自我隔离、拒食等）

1. 如果你状态不佳，希望他人通过何种方式关心你？（例如电

话、短信、上门探访等等）

延伸阅读

- Healing the Fragmented Selves of Trauma Survivors by Janina Fisher
- The Body Keeps The Score by Bessel van der Kolk
- Trauma and Recovery by Judith Herman
- The Shock Doctrine by Naomi Klein
- Surviving by Bruno Bettelheim
- Self As Other: Reflections On Self-Care by Crimethinc.
- Turn Illness into a Weapon by SPK

[image]
[image]

应对创伤：心理安全S08E03

[image] 关键词	互助 创伤 团队 复原力 心理安全 战争 气候灾难 直接行动 自主
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月4日
[image] **Description**	心理安全

有时，只有通过灾难，我们才能发掘出一种无法衡量或定义的力量。

有时，黑暗就是我们的蜡烛。

有时，我们的伤口会照亮我们的道路。

有时，治愈会以迂回的方式发生在我们周围和内心深处。

本集内容专门提供给照护者 —— 帮助他人的人同样需要足够的帮助。在气候危机、人为灾难、战争频发的年代， 我们需要彼此 。

- Table of Contents

  创伤与毒性压力
  理解替代性创伤
  创伤的三种反应
  创伤经历后的可能反应
  为什么有些人能从创伤中恢复，而另一些人却不能？

康复的关键要素
转变创伤的有效行动计划包含三大核心要素：觉察、平衡与联结。
我们能为您做些什么
你能为自己做些什么
如何支持你的朋友
突破与希望

[image]

长期从事高强度的团结工作而不感到情感耗竭是非常困难的。目睹他人的痛苦可能造成情感创伤。每当遇到新案例 —— 每当目睹新的个人悲剧 —— 不公义便如重拳般击打在我们脸上。

基层团结工作要求我们与受助者建立真实的情感联结，这必然使我们暴露于他们的痛苦之中。我们或许总将自身遭遇轻描淡写为微不足道，尽管确实未亲历真正的暴力或损失，但接连不断的故事仍会对我们产生累积性的影响。

无论是飓风卡特里娜后的新奥尔良、巴勒斯坦的人权工作、加莱的难民支援，还是其他无数场景，我们反复见证着：参与援助者常陷入复杂的情绪漩涡 —— 愧疚、羞耻与"低强度累积性"创伤交织缠绕。更常见的是，人们会否认自身症状的存在；即便察觉异常，也认为自己不该"允许"这些感受存在。这些受创者中，有我们的爱人、朋友和激励我们的英雄 —— 我们深知必须在运动中更好地融入疗愈正义理念。

对于那些已作出回应的人，我们理解你们可能因"做得不够"而感到愧疚或羞耻。你们或许会这样想或这样说："当人们正在受苦时，我怎么可能享受快乐和放松？"

未能尽责的愧疚与羞耻感，几乎是每位活动家和每场运动的诅咒。当受苦者是你相识之人、是你所爱之人时，这种感受尤为尖锐。这看似显而易见，却需要反复强调：这不是你的错。

气候混乱、战争与剥削的灾难仍将持续上演。作为基于团结精神的救援工作者，我们必须践行心理健康意识，关怀自我与同伴，方能应对

此类工作领域可能引发的创伤。我们呼吁：即便身处危机时刻，也请将身心健康置于首位。同时请监督我们，确保组织文化始终保持可持续、赋权与互助的特质。

在争取正义与解放的运动中，我们常谈论万事万物的可持续性，唯独忽视了自身。我们可能耗尽自己的"情感储备"，或"日夜操劳"，却期待身心自行修复。但每个人都有崩溃临界点，一旦逾越，可能需要数月甚至数年才能恢复。有些人已认清自身极限，并努力在可承受范围内工作。然而在灾后重建的紧张氛围中，人们可能被逼迫超越自身极限，或被迫要求他人超负荷工作。悲剧的是，这往往导致成员彻底退出运动。

若在激烈的行动中发生这种情况，事后务必留出时间并采取其他措施进行恢复。

[image]

创伤与毒性压力

战斗、逃跑或僵持的防御机制是一种极其强大的反应，在威胁情境中会自动启动。在紧张局势的瞬间，它控制着人的行为。杏仁核 —— 大脑中控制恐惧反应的区域 —— 必须迅速作出反应，因为这类情境被解读为生死攸关之事，仅留下有限的应对选项：战斗、逃跑或僵持。

虽然这种机制通常非常有用且自然，但如果因长期反复暴露于创伤性事件和/或高度压力事件中而过度激活，则可能产生诸多有害影响。创伤事件往往会引发生活困境，进而增加再次触发创伤反应的概率，最终导致所谓复杂性创伤 —— 即个体一生中经历多重创伤事件的状态。毒性压力则源于长期频繁暴露于逆境环境的生存体验。事实上，我们所服务的多数社区正处于此类境遇中，而作为深入这些社区的行动者，我们同样无法免受这种毒性过程的影响。

需特别指出的是，创伤事件的定义因人而异：每个人都有独特的情感体验，应对创伤的方式也各不相同。大脑对创伤的反应呈现出多种形

态。当这种破坏性过程持续存在 —— 尤其在毒性压力环境中被长期强化时 —— 我们与自我认知的联结往往会断裂，创伤由此成为存在性和生理性的双重创伤。

长期处于这种持续压力状态会损害健康，引发多种神经系统与生理反应：免疫系统关闭导致感染风险上升、短期与长期记忆丧失、消化功能障碍等。身心正竭力应对其认定的短期危机，通过集中精力维持基本生存功能来应对。

事后，我们的脑部和身体系统会试图重新掌控局面，并试图理解这段经历以避免重蹈覆辙。大脑可能在我们内心深处不断重播这段经历以试图理解它，与此同时我们却想回避与之相关的任何事物。由于感到不安全且对发生的事情感到痛苦，我们可能会变得情绪封闭。

诚然我们无法完全掌控人生，但通过理解创伤的运作机制并掌握应对技巧，我们能够逐步重拾力量感、完整感与个人效能。此外，在帮助他人度过丧失或危机时，我们既能降低其创伤风险，又能通过这个过程获得对可能性的全新认知。

理解替代性创伤

替代性（或旁观者）创伤是指因你关心受伤害者，并感到有责任帮助他们，而产生的心理变化过程。其影响与前文所述创伤体验几乎相同。随着时间推移，这种过程会导致你的心理、生理和精神健康发生改变。其唯一区别在于：这种创伤并非你亲身经历，而是通过他人创伤体验间接获得。

替代性创伤具有累积性。当你目睹残酷行径、聆听毁灭性故事时，这种创伤便会产生 —— 无论你只听过一个故事，还是日复一日、年复一年地接连听闻诸多故事。这种改变过程持续进行，你的替代性创伤体验不断受到个人生活经历的影响。

替代性创伤的根源在于你的关怀 —— 你对受苦者的共情。你具备同理心：理解他人经历、反应与感受的能力。当你关心那些经历过惨痛

遭遇的人时，他们的悲伤、恐惧、愤怒与绝望便会渗入你的意识，以某种方式与彼此共同感受。

替代性创伤的产生源于你肩负的帮助责任。这是值得肯定的！但可能导致你对自身、他人及期望结果产生极高（有时不切实际）的期许。面对巨大需求与苦难时，你的承诺感与责任感终将演变为沉重负担、不堪重负和绝望的情绪，甚至迫使你超越自身健康边界或你试图帮助的人的长远利益而过度付出。值得注意的是，多次研究表明，无论从事这项工作多久，每个人都会感受到这种影响。

你对团结工作的承诺感和责任感如何帮助你？又可能如何伤害你？

创伤的三种反应

经历直接或间接的残暴与苦难后，人们通常会产生三种不同的反应。这些反应常被称为"创伤后应激障碍"。个体可能经历其中一种、部分或全部反应，具体包括：

1. 创伤事件的再体验：噩梦、闪回、侵入性记忆、无法摆脱经历的感受；

1. 逃避/压抑/情感麻木：记忆缺失、自我药物治疗（酒精等成瘾物品/药物）、自我隔离、社交退缩、回避所有可能唤起记忆的事物（即回避行为）；

1. 警觉性增强：失眠、易怒、暴怒、情绪爆发、恐慌发作、恐惧、过度警觉、注意力涣散及难以完成日常任务。

创伤经历后的可能反应

这些都是极端情境下的常见反应。

你曾经历过哪些迹象？回想一下哪些细节可能是最初警示你开始承受创伤的信号？

你的创伤挣扎同样会严重影响身边亲近之人。退缩、酗酒、失眠、性欲减退、过度保护、丧失同理心或希望 —— 这些都会改变你与所爱之人的互动方式。

不妨向亲近之人询问："当我承受压力时，你注意到我的行为和情绪有何变化？" 或类似的问题。

人们对创伤经历的反应各异，强度也不同，所需的支持方式亦不相同。创伤可能源于亲身经历、目睹事件，也可能因认识幸存者或仅是听闻事件而产生。

对多数人而言，这些症状会在4-6周后逐渐消退。但若持续存在，通常会被诊断为"PTSD"（创伤后应激"障碍" —— 尽管我们反对用"障碍"一词描述这种正常反应）。

此时建议寻求"专业"帮助（若初期反应强烈，专业干预本就值得考虑）。创伤后应激可能在事件发生数月甚至数年后才显现，因为我们最初并未完成创伤体验的消化。当经历被封存时，创伤便持续造成伤害。当情绪过于强烈时，寻求专业帮助绝非可耻之事。但作为行动者社群，我们同样需要践行治愈正义与社群关怀，创造能让集体同理心与宽容发挥作用的空间，从而减轻创伤体验（无论是亲身经历还是代偿性创伤）带来的影响。

[image]

为什么有些人能从创伤中恢复，而另一些人却不能？

以下这些因素似乎会增加一个人患上创伤后应激障碍的可能性：

- 创伤越严重
- 持续时间越长
- 当事人越接近创伤现场
- 创伤看起来越危险
- 如果创伤是由他人故意造成的（例如警察和狱警的暴行）
- 创伤经历次数越多
- 如果当事人获得亲友的负面反应 —— 这正是我们更需有效相互支持的原因
- 事后进入安全/受支持环境所需时间越长 —— 最初的几分钟至几小时至关重要。

然而必须强调：每个人经历创伤情境时的反应各不相同，面对创伤事件没有绝对的对错之分。最关键的是牢记：信自己。如果某件事让你感到创伤，那么它就是创伤。

康复的关键要素

1. 在安全环境中静心片刻。确保待在一个能让你感觉平静的地方，有安全感的地方，身边有值得信赖的且能关怀你的亲友。

1. 梳理经历。用语言描述发生之事。向朋友详述经过。记录事件始末。选择适合自己的方式表达。

1. 实践积极应对策略。积极应对策略有助于自我照护 —— 尤其是逃避、休息和娱乐。

积极应对策略示例包括：阅读书籍、观影、玩电子游戏、与朋友聊工作之外的话题、休假放松、草地躺卧、品茗小憩、午睡休憩、按摩放松、体育锻炼、分享趣事、进行创作。关键在于找到最适合自己的方式，切勿盲目效仿他人。

哪些你喜爱的活动能帮助应对创伤？

然而我们不仅要应对创伤，更要实现疗愈与蜕变。创伤转化意味着寻找滋养意义感与希望的方法。

具体方式包括：重申工作价值、维系亲友联系、关注生活细节、延续传统仪式、阅读写作、祈祷冥想、挑战消极信念、持续学习、记录心绪、进行艺术创作。

哪些你喜爱的活动能助你更深层地转变创伤？我们想要的不只是应对。我们想要疗愈和转变。转变创伤意味着找到培养意义感和希望感的方法。

转变创伤的有效行动计划包含三大核心要素：觉察、平衡与联结。

- 觉察

理解自身反应及其成因，能帮助你明确需求，从而改变现状或管理情绪反应，避免事态恶化。在行动时保持觉察，有意识地让身心保持同步，有助于预防或管理创伤。

反思自身感受（身体、情绪、精神层面）。是否察觉到异常？如果有，可能跟何种因素相关？

- 平衡

努力平衡个人需求与工作需求，平衡高强度任务与低强度任务。确保每日工作包含用餐/运动/休息时段。花一些时间与你不必照顾的人在一起，或者更好的是，与照顾你的人在一起。

理解精疲力竭的活动家和志愿者容易犯错，可能适得其反。

请填空："我有时难以平衡___与___。"

- 联结

维系滋养人心的关系与有意义的社交，是应对替代性创伤的最佳方式之一。

联结也意味着与滋养你、锚定你内心的事物保持连接 —— 无论是自然、宗教，还是其他赋予你意义、敬畏、喜悦、惊奇、目标与希望的源泉。这同样至关重要。

哪些社群能让你感受到滋养、支持与联结？

对工作的认知方式，对保持身心平衡、预防或管理创伤至关重要。请自问：

- 你为何从事这份工作？
- 你的工作如何契合互助救灾组织的大局/使命，或更广泛的气候正义愿景？
- 你如何衡量工作成效？

- 工作中哪些要素可由你掌控？

- 这项工作带来哪些代价、回报是什么？你个人经历了怎样的转变？

- 在严峻情境中，你是否注意到决心、智慧、同情心、勇气、韧性、英雄主义等品质的闪现？

[image]

我们能为您做些什么

我们致力于将疗愈正义融入工作的方方面面，构建相互关怀与体恤的组织文化。我们鼓励所有参与者共同探讨并反思救灾经历。小组成员可依次发言，让每个人都有机会讲述亲历事件、所在位置、所见所闻、感受与思考。

参与完全自愿，且创伤程度相近者交流效果更佳。

[image]

当同伴支持不足以解决问题时，全年无休的免费多语种"灾难心理援助热线"可提供危机咨询与支持，帮助因自然或人为灾害遭受情绪困扰的人群。还可以拨打1-800-985-5990或发送短信"TalkWithUs"至66746，即可联系专业危机咨询师。

互助救灾组织在支持您降低创伤风险或缓解创伤影响方面有哪些优势？还有哪些改进空间？

你能为自己做些什么

照顾自己并非自我放纵，而是自我保全，这本身就是

一场政治斗争。——奥德丽·洛德

- 寻求安全

经历事件后立即前往安全场所，照顾好自己。这可能意味着允许他人照顾你。

切勿自我封闭。

向朋友倾诉并明确表达需求。亲友往往不知如何帮助，请告诉他们你需要什么、不需要什么。

- 行动起来

释放体内残留的肾上腺素：散步、骑车、跑步或做运动。

- 自我提醒

你可能因发生的事感到内疚自责。请时刻提醒自己：这不是你的错！你的反应很正常，且有专业支持可寻；这是艰难阶段，但你会好起来。

深入了解创伤机制。认知越充分，越能将自身反应视为对"异常事件"的正常反应。

- 警惕不健康的应对机制

逃避和否认长期会造成伤害并限制生活。

酒精药物自我治疗看似缓解，实则长远有害。滞留于不健康关系中亦是如此。

- 探索替代方案

巴赫花精疗法和针灸可助情绪调节。缬草根有益改善失眠。按摩与热水浴始终是良策。

如果想要寻求专业帮助，请勇于寻求。优秀的治疗师或其他专业人士能提供帮助。务必选择让你感到安全、愿意敞开心扉的对象。如果对方在政治立场上持同情态度或至少保持中立，将更有助益。正如腿部骨折需要就医，创伤也是真实存在的情感痛楚。

- 承认

你已做过、正在做或打算做的事。即便短期成果看似微不足道，也应视作漫长抗争的阶段性胜利。遗憾的是，在可预见的未来，灾难和灾难投机者仍将存在 —— 他们企图借灾难巩固权力与特权。你的精疲力竭既无法改变现状，也无助于受助者。我们都需要探索避免倦怠与自责的方法。

- 结伴同行

带着值得信赖的伙伴出发，或在当地寻找能共同工作、休息和娱乐的伙伴。结伴虽非万全之策，但正如许多人都知道的那样有人守护在侧便能获得莫大慰藉。更理想的是组建完整团队。

我们倡导 亲密团队组织模式 ，其优势之一在于能 形成相互关怀的微型生态系统 。

- 不要拿自己和他人做比较

倾听内心的声音，关注身体健康。世上极少有人能在高压环境下持续多年超负荷工作却几乎不受影响。如果你觉得他人比自己更能承受某种经历，可能会感到沮丧。请记住：每个人都是独特的，反应方式也各不相同。没有所谓的"正确"反应方式。（如果曾经历创伤事件，包括童年虐待，你的反应可能更为强烈。）

此外，敏感者往往反应更强烈。遭受攻击后感到痛苦并非软弱的表现。如果你正想着"我没有资格这么难受 —— 我的遭遇和X相比根本不算什么"，请提醒自己：你经历了可怕的事情，你有权感受此刻的情绪。如果你感到痛苦，正因这段经历对你而言是痛苦的。比较残暴程度毫无意义。接纳自身状态，才能更快康复。

- 务必安排休息与娱乐

既要静养也要消遣。放松身心，开怀大笑，随乐起舞，练习武术，走进田园，享受亲密，或尝试BDSM，好好吃饭 —— 做任何能让你愉悦的事，提醒自己生命值得珍惜。

当那些细微或喧嚣的内疚之声潜入思绪时，承认它的存在，微笑以对，并告诉它管好自己的事。

这是一场持久战，只要好好照顾自己，你很快就能重返战场。

- 尽可能减轻生活压力

在恢复前别再接新任务。比如如果会议令你疲惫，且不是必需出席，那就不去了。

- 睡觉！

还有什么比这更反资本主义、更低碳环保、更反消费主义呢？而且完全免费！尽情享受身体所需的这份美好馈赠。

- 保持耐心

用你自己的节奏疗愈身心，对自身保持宽容，不要因情绪反应而自我苛责。心灵创伤的愈合需要时间与耐心，如同肉体伤痕一般。

- 自问

"我是否准备长期坚持？" 如果答案是肯定的，就需诚实地审视当下行为是否利于目标达成。

着眼长远，这是场马拉松而非短跑。

[image]

如何支持你的朋友

亲友的支持至关重要，其重要性无论怎么强调都不为过。（反之，缺乏支持与理解会加剧创伤的持续。）支持缺失可能使反应恶化。这种现象称为"二次创伤"，必须予以高度重视。它涉及"认知崩塌" —— 人们知道执法者和施暴者可能残暴，但如果事后连朋友都不支持你，你可能会觉得整个世界都崩塌了。这就是亲密关系需要介入的时候！

以下是一些帮助你能够支持朋友的建议。

- 坦诚相待

在私下合适的场合，温柔地告知朋友你注意到其行为出现令人担忧的变化。如果这些变化影响到工作效率或人际交往，请务必明确告知。

具体描述可能更有助益。

务必澄清你关注的是当前行为而非"真实的他们"，并强调正是出于深切关怀才提出此事。

带他们外出放松，尽量避免谈论工作。不妨向他们展示本站的心理资源。

- 主动关怀

经历创伤者往往难以主动求助。请主动伸出援手但切忌强迫。

不要等待对方开口求助，要主动陪伴。

创伤发生后的最初几天至关重要，此时情绪最易外露，正是倾诉的良机。

若错过这个窗口，当事人往往会把自己封闭起来，回避社交活动。

如果你发现朋友不再露面，请主动寻找他们。

- 倾听

当事人可能需要反复讲述创伤经历，朋友最能做的就是耐心倾听并给予同理心，让他们感受到陪伴。

避免过早、过长或过多地谈论此事。我们常渴望给予建议，却忘了做好倾听者。

设身处地 —— 尝试理解对方真实感受，而非代入自身感受。

按事件的发生顺序叙述有助于大脑处理创伤。谨慎引导朋友描述所见、所闻、所感与所思。

但如果对方不愿谈论，切勿强求。

- 保持合理的预期

在对方康复期间保持现实的合理预期至关重要，既不要期望过高也不

要期望过低。别指望受创者能迅速恢复。有些人能做到，但有些人做不到。

如果有人从危机中恢复缓慢，请持续给予支持，让他们不觉孤立无援。

- 不要把事情当作针对个人

遭受创伤的人可能出现令周围人难以应对的症状，例如愤怒、退缩、易怒、不知感恩和疏远都是常见的反应。请记住，创伤者并非故意如此行事：正是创伤导致他们表现出这些行为。不要将其视为个人攻击，而应认识到这是症状表现，表明他们需要你的支持。

- 切勿轻视创伤

人们总忍不住劝对方停止沉溺往事，要求其忘却创伤继续生活。遗憾的是，这种建议通常适得其反，反而可能加剧困境，使当事人感到更加孤立无助。

- 提醒朋友

最关键的传递是："这不是你的错——你并不孤单。"

- 保持常态

怜悯或过度溺爱的"过度关怀"无济于事。

最重要的是让朋友在你身边感受到安全与温暖。

- 自我学习

你可能对如何帮助感到不安。多了解创伤知识以加深理解。请记住，

许多人在经历创伤后看似正常，反应可能延迟出现。

请询问对方需求，而非强加解决方案。

- 陪伴支持

创伤者常连日常琐事都力不从心。代为烹饪、购物、处理家务都是无价之助，但切忌居高临下或剥夺其自主权。如果朋友尝试重返示威现场、行动场所或其他可能触发创伤的情境，不妨同行相伴。

全程关注其状态，在活动前、中、后持续询问感受。

此外，当创伤后应激症状消退后，协助朋友重新融入积极生活同样重要。

- 寻求支持

请谨记：支持者同样需要支持。支持支持者至关重要。

帮助与关怀对你而言也可能极具挑战。请照顾好自己，做让你快乐的事。向他人倾诉你的感受。获得自我支持将更有力地支撑你帮助他人。

突破与希望

经历创伤性事件也能最终带来积极的最终结果。许多人曾经历过此类遭遇，不少人表示崩溃最终转化为突破，成为自我成长的契机。例如：学会有意识地享受生活与周遭之美，对每一天心怀感恩。

[image]

直面恐惧并战胜它，能赋予人强大的力量。

更广阔的认知与谦逊之心，能让你成为更具同理心与理解力的人。

而经历过创伤的人，更能洞悉如何帮助他人走出阴霾。

这个世界有太多需要转化的事物，你那饱含心酸、历经磨砺的智慧，正是生死轮回与新生重启的时代所必需的。

永不放弃。世界比以往任何时候都更需要我们。

人有时会破碎，但正是裂缝让光线得以穿透。

这些裂痕昭示着新生正在萌发 —— 是青翠的，是崭新的。

有时唯有灾难才能唤醒我们体内那份无法衡量、无法定义的力量。

有时黑暗便是我们的明灯。

有时伤痕照亮前路。

而疗愈终将降临，以迂回的方式，遍布我们周身，深植我们心底。

— — 要疗愈，我们就必须抵抗；要抵抗，我们就必须疗愈。——

[image]
[image]

走出绝望：心理安全S08E04

[image] 关键词	健全主义 心理安全 抵抗 疗愈 等级制度 自治
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月5日
[image] **Description**	心理安全

只要我们知道正在建设当下力所能及之事，让遥远的未来保持未知也无妨。

- Table of Contents
个人主义的局限
他们不赋权，只吞噬
旅程笔记
1 、未来不存在放之四海皆准的"解决方案"—— 那些将“解放”捆绑于等级制度的方案，终将扼杀解放的可能性。
2、拒绝那些耗尽我们能力、阻碍我们追求喜悦的组织形式，是完全可以的。
3、倾听身体的声音是正当的，为悲伤留出空间、哀悼与疗愈是正当的。
4、为尊重个体有限的承载力而设立边界，是完全合理的。
5、优先与那些已经与你建立了亲密关系、理解你需求的人合作是完全可以的。

[image] [image] 这是伟大的誓言。也将是格外艰难的实践。

个人主义的局限

我们常常因目睹日常压迫而心灰意冷地回到家中。我们渴望做更多事情来对抗助长压迫的惯性。

有时我们能有所作为 —— 但更多时候力不从心。

在本集中，我们将探讨不断撞上能力边界的深层含义，我们想要深入阐述，将压迫定位为“个体可以或应该独自拆解”的观念，是一种陷阱反而维系了我们所反抗的暴力。我们将剖析：当我们渴望改变世界时，为何这种意愿反而被利用 —— 我们的能量不断被导入那些维持现状而非打破桎梏的等级体系，最终使我们屈服。最后，我们将分享如何在前线和后方应对内心的悲伤，并传递我们正在践行的经验。

- 当选择的数量如此之多已超出我们的情感、体力与财力的承受极限，该如何践行"正确之事"？
- 当殖民主义、资本主义与父权制看似势不可挡，我们又该如何应对渺小无力的感受？
- 如果我们只能在自身所能抵达的范围内挣扎求生，在压迫的汪洋中存活又意味着什么？

每一天我们目睹的饥饿者远超自身所能喂养，无家可归者远超所能收容，苦难与伤痛远超所能承受。然而我们也看见货架满溢的食物，可供栖身的建筑空置，以及成千上万本可以携手共建互助世界的民众 —— 却被沦为机器中的齿轮，被迫为最基本需求相互竞争。多数时候我们不禁自问："作为在日常生活中挣扎的个体，我们还能做些什么来打破压迫的惯性？"

本集旨在探讨：将压迫定位为“个体可以或应该独自拆解”的观念，如何是一种陷阱反而维系了我们所反抗的暴力。我们要揭示：当我们渴望改变世界时，如何被诱导用个人选择替代集体行动。我们要命名那些将抵抗力量收编为己用的结构，正是它们制造了当下许多人深陷的绝望。我们期待通过分享经历，挖掘出"力有未逮"时的羞耻感，并将这种情绪转化为呼唤集体关怀与互助投入的号角。

[image]

必须澄清一点，思考自己能做些什么以消除压迫并不是坏事。这是我们抗争的基石，正是通过从自身做起，我们才能真正行动起来。但是，种族主义殖民主义、父权制和资本主义个人主义早已让我们深信：孤立的选择能成为强大的政治行为 —— 尽管事实往往并非如此。仅靠素食主义无法终结统治压迫。购买电动汽车也不能。慈善捐款无法消除贫困。在非营利组织志愿服务或工作也无法根除压迫 —— 事实上，这类机构的设计初衷正是维持现状。投票与政策改良同样无法瓦解警察国家。这些工具从不以终结压迫为目的，其中许多甚至始终旨在瓦解激进运动的力量。

当我们认同"个体及其选择是系统变革主要驱动力"的叙事时，便容易接受这样的结论：我们个人有责任拆解压迫的等级制度，如果失败就该自责。但压迫者深知个体的抵抗无法阻挡他们，于是利用我们的抗争意志反噬我们。如同专为榨取消耗我们全部能量而设的仓鼠轮，他们通过暴力等级制度 —— 例如选举政治、非营利产业复合体、殖民者教育体系 —— 过滤我们的行动，将我们边缘孤立，以确保我们整体的影响力永远无法真正撼动现状。

激进运动永远不被允许跳出转轮，否则必将被强行纳入其中。

如果你认为素食主义或投票等个体选择能“聚合起来”产生系统性变革，我们提醒你：至少在我们社会的语境中，纯素主义和素食主义充斥着阶级主义和白人至上主义。从富裕阶层对贫困人群饮食选择的自满式责难，到全球有色人种穷人为支撑所谓的"有意识消费"而忍受的血汗工厂 —— 资本主义正蓬勃发展。投票亦然。即便各国全民投票，我们仍将生活在种族主义暴力划定的疆界构筑的世界里。

当我们认清资本主义、白人至上主义、父权制、气候变化及其他暴力等级制度的庞大体系时，本该感到绝望。殖民主义的根基在于割裂人与人、人与土地家园、人与自然、人与社群的联结。其力量源于不断重构世界以阻挠个体抵抗的能力。当我们被灌输摧毁压迫的责任“仅在我们肩头”时，我们并非被赋予力量，恰恰相反是被彻底剥夺了能力 —— 使抵抗的念头显得既无力又愚蠢。

日复一日，我们心灰意冷、幻灭消沉 —— 直至精疲力竭。这正是其

终极目的。无论抵抗是被压迫的巨大力量瞬间碾碎，还是被帝国官僚体系日久磨灭，掌权者都企图让我们陷入比任何抵抗意识或集体斗争更深的绝望。

面对日常压迫的沉重，绝望固然是自然反应。但它更应 成为行动号角，催生出超越个体、更强大更坚韧的抗争运动。

[image]

他们不赋权，只吞噬

[image]

“对我而言，关键不在于提供任何改善的希望，而在于通过构想一个具有说服力的替代现实，将我的思维 —— 以及读者的思维 —— 从那种懒惰而怯懦的思维惯性中解放出来：即认为当下生活方式是人类唯一生存方式的思维。正是这种思维惯性，让不公的制度得以存续而无人质疑。想象力的运作对既得利益者构成威胁，因为它能揭示现状并非永恒、普世或必然。"—— 厄休拉·勒古恩

前文我们聚焦于揭露个人主义的陷阱 —— 这种被用作延续压迫的工具如何催生慢性倦怠与绝望。

接下来将分享我们在等级制度中组织抗争的亲身经历 —— 这些制度恰恰再生产了我们试图对抗的压迫，而这些经历如何重塑了我们开展运动工作的方法。

第三部分我们将探讨在穿越绝望时汲取的教训，以及如何通过投入时间、精力和物质资源，投身于我们坚信能为自己和所爱之人带来喜悦的世界建构实践。

- 如果解放的梦想永远被推向更遥远的未来，向人们展示悬置的梦想有何意义？
- 如果我们持续且可预测地同意追随，这会赋予所谓的“领导

者”和机构多大的权力？

- 这种权力如何被用来操纵我们，迫使我们做那些阻碍自由、扼杀解放新路径的行径？

在投身自治组织之前，我们中有些人也曾参与选举活动。但当我们逐渐看清选举过程中的腐败、不负责任和政治投机时，便对此深感厌恶。我们认为权力必须更贴近参与斗争的人民，于是转向基层组织工作。然而我们遇到的左翼先锋派，只对能助其夺取国家或殖民主义权力的“事业”感兴趣。我们深切体会到被先锋派"领导层"支配的无力感 —— 他们决定何时组织、如何组织、与谁组织以及推进速度。我们意识到这并非我们所追求的解放 —— 这根本不是解放，而是用一个新的管理阶级取代旧的，他们同样热衷于剥削我们。

与此同时，我们中许多人供职于表面宣称致力于"打破贫困循环"的非营利机构。然而像我们这样的直接服务人员领着贫困线水平的薪资，而"创始人"和管理者却获得远高于我们的报酬；我们对公平正义的热忱被利用来胁迫和内疚感逼迫我们付出超出承受极限的努力；从一开始，我们就背负着个人能力无法企及的不合理期望。

在选举、先锋派和非营利机构这三类经历中，我们不断追问相同的问题：这些组织模式有何共通之处？为何在其中穿行时，我们总感到如此无力、疲惫与悲伤？

政客、先锋派和非营利组织都试图将斗争纳入各自对未来的构想。其逻辑是：房屋必须有主人，运动就必须有领袖。当然，在构建他们的未来时，我们常常被要求成为"事业"的牺牲品。多年后，我们逐渐看清最常见的组织形式都是自上而下的模式，痴迷于追求规模效应（尽可能覆盖更多人群）。但当规模成为组织的核心目标，它便要求我们忽视自身需求与能力，并强化了将我们与其他抗争者割裂的等级制度。

我们陷入慢性疲惫和悲伤，因为无论付出多少努力，永远无法达到被要求达到的规模。我们筋疲力尽，因为我们的组织方式没有考虑到我们自己的需求。最终，这场组织活动既非为我们自身的解放，也非为我们所认识和珍视之人的解放而存在。我们为虚幻而僵化的"群众"牺

牲自我，为他人严苛定义的革命牺牲自我，为某些领袖所谓"真正的工作"牺牲自我 —— 这些定义总将我们自己的需求置于次要地位，或压制我们寻求支持的诉求。对我们而言，这种状况必须改变。

但在改变组织方式之前，我们必须先转变对未来的认知。我们必须学会对那些没有被监禁国家、非营利产业复合体或殖民想象预先勾勒的可能性保持开放。我们必须审视自身关于规模与革命的政治立场。我们必须质疑在等级体系中组织行动的意义，必须正视我们及所爱之人承受的种种苦痛。

我们如今认识到，与那些我们努力扶持的人之间的界限，若非虚幻，也纯属人为划分。我们曾是（且仍是）抗争者。我们曾生活（且仍在）于住房与医疗保障的困境中。我们曾是（且仍是）我们为之解放的对象，因为我们曾是（且仍是）被压迫者。

[image]

旅程笔记

> “我坚信，你的政治立场如果不能具有解放性并因此带来喜悦，就必然存在问题。我自己也经历过‘悲伤政治’的阶段，学会了识别导致这种情绪的错误根源。其成因多种多样，但关键因素之一在于我们总会夸大个人能力的重要性，以致于因成就不足而深陷愧疚。” —— 西尔维娅·费代里奇

我们希望分享一些经验教训，这些经验帮助我们在被迫奔忙的间隙创造出更多可能 —— 并期待能让我们更接近某种可持续的状态。

这些经验是指导原则而非硬性规则。它们或许能引起你的共鸣，也可能不然。我们从未试图宣称某种方案适用于所有运动空间和建设者 —— 自治主义者与无政府主义者都明白，那将立即在组织中引入等级制度，违背我们毕生奋斗的信念与实践。

请阅读这些文字，分享它们，愿你从中找到共鸣。

- 如何建立尊重个体存在的边界，让我们在集体斗争中保有自我？
- 如何平衡抗争工作，为生活的夹缝留出空间？
- 如果我们自己都不属于人民，人民的革命又为谁而战？

当人们了解我们作为自治主义者的政治立场时，常会问："那我们该做什么？" 有时提问者心怀不轨—— 他们深知不可能给出完整答案。他们往往预设了成败标准 —— 取决于我们的答案是否符合他们自己对变革的想象。他们早已执着于单一的未来，而非通过多元路径实现解放的可能性。

在其他情境中，我们明白这个问题源于绝望：当我们已经付出了如此巨大的牺牲，还能奉献什么？

我们希望避免在反抗方面开出任何简单的药方：我们不是领导者，也不是未来的预言家。我们在这里能提供的，是迄今为止我们学到的经验教训。

只要我们知道正在建设当下力所能及之事，让遥远的未来保持未知也无妨。

1 、未来不存在放之四海皆准的"解决方案"—— 那些将“解放”捆绑于等级制度的方案，终将扼杀解放的可能性。

我们必须挑战自我，将未来视为对可能性的向往，而非执着于那些非我所建、亦不以解放为宗旨的制度体系的"成败"。

于我们而言，我们开始追问：

[image]

如果未来的微小部分已经与现在并存了呢？

如果人们已经在自主组织了呢？我们能和他们联结起来吗？

本土有没有自治组织的历史？

如果我们的未来不那么依赖遥远的事物，而更多地依赖于我们如何好好地培养我们所生活的边缘中存在的事物呢？

2、拒绝那些耗尽我们能力、阻碍我们追求喜悦的组织形式，是完全可以的。

所有资本主义机构本质上都带有健全主义倾向。由此延伸，那些未摆脱资本主义工作伦理的组织空间，注定无法实现可持续运作。

它们设定的期望只会催生倦怠，并复制着它们声称要摧毁的剥削模式。若我们开始视自己为值得解放的存在 —— 而非解放斗争中可随意消耗的工具 —— 那么拒绝那些不断要求我们自我牺牲的组织形式，便是理性的选择。一切解放斗争都是为生命、喜悦与联结而战 —— 而非绝望与死亡。

3、倾听身体的声音是正当的，为悲伤留出空间、哀悼与疗愈是正当的。

我们的身体承载着祖先的集体智慧。通过倾听身体，我们能开始打破殖民主义、白人至上主义和父权制的残障歧视。当我们感到疏离时，身体在提醒：建立共同体关乎个体和集体的生存。当我们精疲力竭时，身体在宣告：仅凭一己之力无法完成所有使命。当我们萌生退意时，身体传递的休憩需求，同时昭示着我们需要这样的抗争共同体 —— 当我们需要退后疗愈时，他们能挺身接力。

4、为尊重个体有限的承载力而设立边界，是完全合理的。

无论我们做什么，通常都存在多个正确选择 —— 而作为个体，我们无法面面俱到。

压迫并非由单人制造，我们也不该指望个人去终结它。

当我们对自身或微小抵抗社群要求过高时，便在重演压迫者的世界 —— 因为我们复制了滋养压迫的健全主义。若感到渺小或孤立，这并非证明个体无力改变，而是昭示着社群联结的必要性。

唯有建立这样的空间，我们才能作为共同抗争的集体，充分释放潜能。

5、优先与那些已经与你建立了亲密关系、理解你需求的人合作是完全可以的。

我们常被要求作为激进分子去"激进化民众"—— 却鲜少顾及自身心理健康与承受力。

但在等级与支配充斥的世界里，根本不存在真正安全的空间。我们绝大多数时间都在周旋于持有有害观点的人群中，与之互动，并寻找微小的抗争方式。家人、同事、街头行人 —— 多数人的观点与我们相悖，正在伤害我们。但我们被迫与这些人周旋，因为拒绝意味着遭受惩罚、失去生计、暴露身份并成为攻击目标。

我们始终在做着这份工作，只因别无选择。

所以，设立界限怎么会对我们的安全和理智毫无意义呢？刻意选择那些我们真正想要一起共事的人 —— 那些想和我们一起共事、尊重我们的时间和完整自我的人 —— 有什么错呢？选择那些真正给我们的生活带来意义、与我们共度时光是有益而非有害的人，又有什么错呢？

正是这些人向我们证明：相互体恤才是最持久的抵抗形式，我们无需"成功说服大众"或者牺牲自我就能创造实质性的改变。

在彼此共建的历程中，我们正昭示着更美好的世界不仅可能发生，更是正在发生。

[image]
[image]

掌控焦虑的策略：心理安全 S08E05

[image] 关键词	主导情绪 人际安全 原子化 反叛 战术 抵抗 焦虑 行动 资本主义
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月7日
[image] **Description**	心理安全

如今，几乎每个人都深陷焦虑。

本集将要展示的是关于焦虑的六点论题，以及焦虑为何能有效抑制了抗争情绪，以及克服焦虑的一种可能策略。

- Table of Contents

  1：资本主义的每个阶段都存在其主导的反应性情感
  2：当代的抵抗诞生于二十世纪六十年代的浪潮，是对主导情感“无聊”的回应。
  3：资本主义在很大程度上吸收/收编了对抗无聊的斗争。
  4：在当代资本主义中，主导性的反应性情感是焦虑。
  5：焦虑是公开的秘密。
  6：当前的策略理论已失效。我们需要新的策略理论来对抗焦虑。
  7：需要一种聚焦于不确定性的新型意识觉醒。
  1、基于经验产生新的实证理论。
  2、承认经验的现实性与系统性。
  3、情感的转化。
  4、创造或表达“声音”。
  5、构建去异化的空间。

6、基于经验的相似性来分析并理论化结构性根源。
“顿悟”与实践的益处
助益
挑战和对策
后记：原因与情感
【转评论 —— 2026/0325】

[image]

1：资本主义的每个阶段都存在其主导的反应性情感

资本主义的每个发展阶段都存在维系其运转的特定情感。这种状态并非静止不变。某种“主导情感”的盛行仅能持续至足够瓦解该情感及其社会根源的抵抗策略被制定之时。这就是为什么资本主义不断陷入危机继而又围绕“新”主导情感重组。

[image]

每个阶段，主导情感都是“公开的秘密”，这正是它所需要的特征之一 —— 因为，只要主导情感保持“公开秘密”的状态，其效力就能持续存在，对抗策略就更难以萌生。

公开秘密往往被个人化。“问题”被视为仅在个体心理层面显现，其社会根源则被掩盖。 每个阶段都将制度造成的苦难归咎于制度的受害者 - 而不是制度本身，并将自身功能逻辑的核心部分描绘成“偶然的局部问题”。

在现代时期（直至战后秩序确立前），主导情绪是“苦难”。十九世纪的主流叙事宣称资本主义将带来普遍富裕，而其“公开秘密”正是工人阶级的苦难。

革命者揭露了这种苦难，十九世纪第一波现代社会运动正是对抗苦难的武器。罢工、工资斗争、政治组织、互助会、合作社及罢工基金等战术，通过确保一定程度的社会最低保障有效击溃了“苦难”的统治力量。其中部分策略至今仍然可以用来对抗苦难。

当苦难失效后，资本主义转向以“无聊”作为控制手段。

二十世纪中叶的主流叙事宣称：生活水平正持续提升 —— 消费、医疗与教育资源的获取渠道不断拓宽。富裕国家“全民幸福”，贫困国家正迈向发展。而这里公开的秘密是：人人都感到无聊。这是福特主义体系的产物 ——该体系盛行至1980年代，以终身全职工作、保障性福利、大众消费主义、大众文化为基础，并收编了原本为对抗苦难而建立的劳工运动。

工作保障和福利供给消解了焦虑与困苦，但工作本身枯燥乏味，充斥着简单重复的劳动。世纪中叶的资本主义提供了“生存”所需的一切，却扼杀了“生活”的可能性；这套体系如同强行灌食般将生存需求填充至饱和状态。

当然，并非所有福特主义下的劳动者都享有稳定工作或保障 —— 但这仍是核心工作模式，整个体系皆围绕其构建。该阶段存在三种劳动契约，其中妥协式B级工人契约 —— 以枯燥换取保障 —— 最能体现福特主义与无聊的结合。如今B级工人契约已基本消亡，而**A**级与**C**级工人之间形成了巨大的鸿沟 —— 前者是消费社会的内部成员 - 高薪的中产阶级“创意阶层”，后者则处于边缘地带，享有自主权却缺乏保障 - 零工工人和底层流民。

[image]

2：当代的抵抗诞生于二十世纪六十年代的浪潮，是对主导情感“无聊”的回应。

如果每个主导系统的每个阶段都存在主导情感，那么每个抵抗阶段都需要针对性的战术以击败或消解这种情感。

如果第一波社会运动是抗击“苦难”的机器，那么第二波运动（1960-70年代，或更广义地/且较为松散地指1960-90年代）便是抗击“无聊”的机器。正是这波浪潮孕育了我们自身的运动，至今仍深刻影响着我们大多数的理论和实践。

这个时代多数策略旨在逃离 "工作-消费-死亡" 的循环。

情境主义者率先提出一系列对抗倦怠无聊的策略，宣称 "我们不愿生活在这样的世界里：为确保免于饿死，却必须接受死于无聊的风险"。自治主义通过反工作运动对抗无聊 —— 既在劳动内部（采取破坏和怠工的躺平战术），也对抗工作本身（消极怠工和辞职）。

这些抗争形式与更广泛的社会进程相呼应：反文化群体正集体逃离主流的枯燥劳动与乏味社会角色。

在女性主义运动中，"家庭主妇病态"于1960年代被理论化为系统性问题。随后通过意识觉醒运动，以及由此衍生的文本与行动（从《阴道高潮的神话》到红袜子组织堕胎公开讨论会），揭示出更多深层的不满。类似倾向可见于受压迫者剧场、批判教育学、主要直接行动模式（狂欢式、激进式与和平主义式），以及直至1990年代的运动 —— 如自由派对运动、夺回街道运动、DIY文化和黑客文化。

[image]

返回：

返回：

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

返回：https://iyouport.substack.com/p/--690?utm_source=publication-search

世纪中叶从"苦难"转向"无聊"的认知重塑，对新一轮反抗浪潮的兴起至关重要。我们正处于这波浪潮的尾声。正如第一波浪潮的战术在对抗“苦难”时依然有效，第二波浪潮的战术在对抗“无聊”时同样奏效。困难在于我们鲜少将无聊视为主要敌人 —— 这正是激进抵抗陷入当前困境的根源。

[image]

3：资本主义在很大程度上吸收/收编了对抗无聊的斗争。

对抗无聊的斗争已部分被收编。资本主义推动人们逃离工作空间，创造出“社会工厂”—— 一个将整个社会组织成工作场所的领域。朝不保夕的动荡不安被用来迫使人们回到工作岗位，而劳工领域已扩展至涵盖整个社会工厂。

此类追求的实例不胜枚举：

- 企业采用扁平化管理模式，煽动员工不仅要管理工作，更要将灵魂投入其中；
- 消费社会如今提供更广泛的利基产品与持续性分心的各种东西，其受大众品味制约的程度已不如以往；
- 电子游戏和社交媒体等新产品要求个体投入更高程度的主动参与，并提供去社会化的刺激体验；
- 工作场所通过微差异化、绩效管理以及资本主义边缘地带临时工和半自雇岗位的激增，实现了体验多元化；
- 资本主义催生了媒介化的次级身份的增长 —— 通过社交媒体、显性消费、和终身学习塑造的自我形象 —— 这些身份需要被强迫性地维系。

早期各种抵抗形式已被收编，或在原初形态消亡后以 阉割形式 复活：例如 商K夜店和音乐节取代了真正的 狂欢派对 。

[image]

返回：https://iyouport.substack.com/p/5f7?utm_source=publication-search

[image]

4：在当代资本主义中，主导性的反应性情感是焦虑。

当今公开的秘密是：人人都深陷焦虑。

焦虑已从原先局限的领域（如性欲）、蔓延到了整个社会场域。所有形式的激情、自我表达、情感联结、当下体验与享乐，如今都浸透着焦虑。

毫不夸张的说焦虑已成为从属关系的枢纽。

焦虑的社会根基之一，是无孔不入的多维监控网络：国安局国安部、CCTV摄像头、绩效考核、就业中心、监狱特权体系、对幼龄学童的持续测评分级 …… 但这个显而易见的网络仅是外壳。

[image]

我们需要思考新自由主义的“成功”理念如何将这些监视和操控机制 植入到了 大多数人的主体性与生命叙事之中。

我们需要思考人们 通过社交媒体、显性消费、和舆论场中的 站队（极化） ，进行刻意且表面自愿的自我暴露时，如何 在虚拟“他者”的永恒凝视中 演绎着 表演 。

我们需要思考这种凝视如何扭曲我们彼此发现、衡量与认知的方式 —— 作为永恒表演中被无限监视的共同演员。我们在表演中的成功与否，进而影响着从获取人情温暖到获取生存资源的种种能力，不仅体现在工资形式，更体现在信贷形式。随着公共空间被官僚化与私有化，以及越来越多的人类活动因风险、安全性、滋扰、生活质量或反社会行为而被定为犯罪，媒介监控领域之外的领域日益封闭。

[image] BACK

在这个日益“证券化”与“可视化”的领域中，我们被强制要求沟通。不可沟通的人被排除在外。由于人人皆可被抛弃，系统随时威胁着强制断开任何人的联结 —— 在替代方案已被预先封锁的语境中，强制断联意味着去社会化，最终导致荒谬的别无选择：在去社会化的包容与去社会化的排斥之间徘徊。

这种威胁在当代规训实践中以细微形式显现 —— 从"隔离"和网络禁令，到解雇威胁和福利制裁 —— 最终演变为监狱中严酷的单独监禁。此类制度是焦虑控制的零度形态：在持续危险环境中瓦解所有联结坐标，以致人格崩塌。

[image]

当下主导性的焦虑情绪亦被称为"不确定性"。

这种不安全感将人视为可抛弃的东西以实施控制。

与赤贫的区别在于：生存必需品并非完全缺失，而是附带条件地被剥夺。

[image]

不确定性导致普遍的绝望感；身体持续处于亢奋状态却无法释放。越来越多的年轻人选择与父母同住。相当比例的人口在服用抗抑郁药物。出生率持续下降，因为不安全感使人们不愿组建家庭。在日本，数百万年轻人终日闭门不出（即"隐居族"），而另一些人则以流行病般的规模将自己累死。调查显示半数人口正经历收入不安全。经济层面，焦虑体系的特征包括：精益生产、金融化及其衍生的债务奴役、高速信息流通与资本外流，以及生产的全球化。呼叫中心等工作场所日益普及，员工时刻自我监控，竭力维持"服务导向"，既要承受通话数量的量化考核，又面临持续考核和潜在解雇风险 —— 多数人甚至无法获得正式职位（需工作六个月才能转正）。“形象管理”导致官方规则与现实操作的鸿沟空前扩大。而911事件后的政治气候，更将这种普遍焦虑导入了全球政治领域。

[image]

返回：https://steemit.com/life/@iyouport/3l9d8t

返回：https://steemit.com/life/@iyouport/2iqpnp

返回：https://nodebe4.github.io/oped2/2017-09-12/%E7%99%BE%E5%BF%A7%E8%A7%A3%E6%97%B6%E4%BB%A3-%E4%B8%89-%E4%BB%A4%E4%BA%BA%E6%B2%89%E8%BF%B7%E7%9A%84%E5%B9%BF%E4%B9%89%E5%8C%96%E8%87%AA%E6%9D%80-iYouPort/

[image] “囤满三周”？…… 为什么不吃新鲜的呢？…… 一个典型的用危机感伪装安全感的广告。

5：焦虑是公开的秘密。

过度焦虑和压力是公开的秘密。然而即便被提及、被摆上台面讨论，它们 也经常仅仅被(错误的)视为“个人心理问题”，往往归咎于思维模式缺陷或适应能力不足 。

主流公共话语事实上是在暗示人们“需要”更多压力，以维持"安全"（通过证券化）和"竞争力"（通过绩效管理）。

每次道德恐慌、每次新的镇压或新一轮压制性的法律，都会加剧过度监管引发的焦虑和压力。

人类真实的不安全感被导向助长证券化。这形成了恶性循环，因为证券化恰恰加剧了最初引发焦虑的根源性条件 —— 即随意处置性/用后即弃、大规模监控、高强度的密集型监管。实质上，"国土安全" 被用作为 "自我安全" 的替代品。此类现象早有先例：幻想着以“国家伟大”来弥补个人苦难，以全球战争宣泄“无聊”引发的挫败感。

延伸：https://iyouport.substack.com/p/--f9b?utm_source=publication-search

返回：

[image] 有钱又怎么样？硅谷白人男也开始流行整容拉皮。资本主义健全主义让他们对自然生理也充满焦虑。

焦虑亦被向下转移。人们对生活失去掌控，便陷入强迫性挣扎 —— 通过微观管理可控事物来夺回控制权。例如育儿管理技巧被宣传为能提供明确操作指南、从而减轻父母焦虑的方案。在更广的社会层面，不确定性引发的潜在焦虑催生了强迫性的社会规制与控制项目。这种潜在焦虑正日益投射到少数群体身上。

焦虑正通过多种方式被个人化 —— 从新右翼话语将贫困归咎于穷人，到当代疗法将焦虑视为神经失衡或思维失调。还有百般"管理"话语 —— 时间管理、情绪管理、育儿管理、自我品牌塑造、游戏化 —— 向焦虑主体兜售“可控”的幻觉，以换取对资本主义主体性模式的更大程度的顺从。

[image]

更多归咎替罪羊与犯罪化的论述，将生存困境归因于个人偏差、不负责任或病态自我排斥。这些话语试图维持福特主义的上层建筑（民族主义、社会整合），却剥离其基础设施（国民经济、福利保障、全民就业）。

个人责任论成为这场反扑的核心，强化了脆弱性和对人的可抛弃性。

再看“自我价值”产业 —— 媒体洪流不断灌输通过积极思维实现成功的“成功学”理念，仿佛焦虑与挫败的根源纯属虚妄。这些现象揭示出将问题私人化的趋势，无论是工作相关还是心理层面的困境皆然。

[image]

我们此前指出：公开秘密的运作必须建立在社会孤立/即原子化的基础上。当前的情境正是如此：真实的交流日益罕见。尽管沟通渠道比以往任何时候都更加密集，但交流却日益受制于系统中介。因此在诸多层面，人们被剥夺了实质性交流的可能性 —— 即便系统要求所有人保持联结与可沟通。人们既顺应交流要求而不是表达自我、又在媒介空间中自我审查。

同样地，情感劳动非但无法缓解焦虑，反而加剧了劳动者的痛苦，却仅能转移消费者的注意力（研究表明，强迫劳动者伪装快乐会引发严重健康问题）。

沟通的数量无关紧要。除非存在能言说“公开秘密”本身的渠道，否则解放性社会力量的重组 —— 即重新联结 —— 永远无法实现。从这个意义上说，人们本质上比以往任何时候都更加孤独。对多数人而言（包括许多激进分子），承认自身经历和感受的真实性都极为困难。仿佛事物必须被量化或媒介化（虚拟传播），或被我们预先认定为政治性存在，才能获得真实性的验证。“公开秘密”不符合这些标准，因而始终处于隐形状态。

[image]

6：当前的策略理论已失效。我们需要新的策略理论来对抗焦虑。

[image]

在动员时期和有效社会变革期间，人们会感受到一种赋权感、表达自我的能力、真实感，以及摆脱压抑或异化的状态 —— 这些体验能有效治疗抑郁症和心理问题，堪称一种巅峰体验。正是这种体验维系着政治活动。

然近年来此类体验已变得极为罕见。

我们可聚焦两个相关现象：先发制人和程序性惩罚。

先发制人策略旨在扼杀抗议萌芽，或使其无法产生实质影响。围困战术、大规模逮捕、拦截搜查、封锁管制、入室搜查及预防性逮捕皆属此类。

[image]

返回：https://iyouport.substack.com/p/853?

utm_source=publication-search

返回：[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

返回：https://iyouport.substack.com/p/5-9e6?utm_source=publication-search

返回 -镇压手段：身份检查 ；抄家

程序性惩罚则通过滥用本应服务于其他目的的程序，将人置于恐惧、痛苦或脆弱境地 —— 例如以破坏日常生活的保释条件限制候审者的行动，利用禁飞名单和边境拦截名单骚扰已知的异见者，实施暴力拂晓突袭，不必要地将当事人的照片刊登于媒体、仅依据所谓的嫌疑（有时配合“抓人指标”）实施逮捕、使用疼痛控制擒拿技法，或暗中透露某人正受监控。一旦对国家干预的恐惧被灌输，它就会被网格化分布于公共空间的可见监控网络所强化，而这个网络则充当了创伤和焦虑的战略性触发器。

大量轶事证据揭示了此类手段的恐怖后果 —— 有人因多年等待审判而精神崩溃（即便最终被判无罪），有人在数月与亲友失联后自杀，有人因遭受虐待而不敢出门。这些影响与国家杀戮或强迫失踪行为同样真实，却被刻意掩盖。此外，许多激进分子同样承受着不稳定就业和惩罚性福利制度的压迫。我们未能逃离普遍存在的焦虑生产机制。

[image]

如果说第一波运动提供了对抗“苦难”的机器，第二波运动提供了对抗“无聊”的机器，那么当下我们需要的是对抗“焦虑”的机器 —— 而这正是我们尚未拥有的。

如果我们仍困于焦虑的视角，便未能实现情境主义者所说的"视角逆转" —— 即从欲望而非权力的立场出发。

当今主要的抵抗形式仍源于对抗无聊的斗争，而随着焦虑取代无聊，

这些形式已然失效。

[image] BACK https://t.me/iyouport/14610

当前的武装抵抗运动既无法也无力对抗焦虑。这种抵抗往往涉及刻意暴露于高度焦虑的情境中。起义者通过将负面情绪转化为愤怒，并借助攻击性投射情感来采取行动以发泄这种愤怒，从而克服焦虑。

从许多方面来看，这为焦虑提供了替代方案。然而，人们很难从焦虑直接过渡到愤怒，而创伤经历又容易使人反向退缩。

我们注意到起义者存在一种倾向：拒绝正视心理障碍对激进行动的阻碍。他们的回应往往是"行动起来！" 但焦虑是真实的物质力量 —— 绝非虚无缥缈的幽灵。诚然，其根源常植于精神创伤，但摆脱精神桎梏的问题，绝非简单地通过意识否定就能解决。幽灵的幻象力量背后，存在着一系列心理阻碍，其本质是反应性情感的作用。这种情况下喊"行动起来"，无异于对瘸腿者喊"快走"。

处境看似绝望而无法逃脱，实则不然。这种感受源于不确定性的效应——持续的过度压力、时间被压缩成永恒的当下、个体因疏离（或被系统强行中介）而脆弱、社会空间各层面都在遭受系统的支配。

[image]

从结构上讲，这个体制本身脆弱不堪。依赖焦虑不过是权宜之计，当更强有力的顺从手段失效时才会启用。

系统试图通过让人们感到无力来维持运行，这使得它容易遭受突然的断裂和反抗大爆发。

那么，我们该如何摆脱这种无力感？

[image]

7：需要一种聚焦于不确定性的新型意识觉醒。

为应对焦虑情绪，我们需要重回设计阶段。

必须自下而上构建全新的知识体系与理论框架。

为此，我们需要激发大量讨论，使当下处境的体验与变革理论产生密集的交汇。我们需要在所有被排斥和受压迫的阶层中启动这样的进程 —— 但没有理由不从自身开始。

在探索此类实践的可能性时，我们考察了以往类似实践的案例。通过研究20世纪60-70年代女性主义意识觉醒的实践记录，总结出以下核心特征。

1、基于经验产生新的实证理论。

我们需要重新连接当下体验 —— 而非过去的理论。

核心在于：主流假设阻碍/束缚了我们对处境的认知。必须将其显性化（ BACK 战术原理https://iyouport.substack.com/p/31-- ）。重点应聚焦于那些与 "公开的秘密" 相关的经历。这些经历需要被讲述并汇聚 —— 先在群体内部，再走向公开。

[image]

返回 - 案例：https://iyouport.substack.com/p/35a

2、承认经验的现实性与系统性。

验证经验的真实性是其中的关键环节。我们需确认痛苦确为真实的痛苦，所见所感皆属真实，且问题并非仅关乎个人。

有时这意味着要重新审视被忽视或压抑的经历，有时则需挑战将问题个人化的倾向。

3、情感的转化。

人们常被难以言喻的情绪与普遍的糟糕感受所麻痹。这些情绪需要转化为对不公的觉醒，转化为更具聚焦性而非怨恨的愤怒，转化为自我表达的行动，转化为抵抗精神的重燃。

4、创造或表达“声音”。

围绕“公开秘密”的沉默文化必须被颠覆。需要对既有假设去自然化并予以挑战， 驱逐头脑中的警察。

发声行为将真理与现实的参照系从体制转移至发言者，促成视角逆转——以自身视角和欲望而非体制视角去审视世界。

编织多元经历和故事是重获话语权的重要途径，此过程既是阐释也是表达。

5、构建去异化的空间。

此类空间的存在能消解社会隔阂，既提供审视自身生活的批判性距离，也能构筑情感安全网，以尝试蜕变，消融恐惧。

它不应沦为维系既有活动的自助手段，而应成为重构激进视角的阵地。

[image]

6、基于经验的相似性来分析并理论化结构性根源。

重点不在于简单复述经历，而在于通过理论化实现其转化与重构。

参与者通过不同假设映射自身经历，从而改变其主导意义。这通常涉及在经历中寻找与解放理论相关的模式，将个人困境与微小不公视为更广泛结构性问题的症候。由此催生全新的视角、一种动机词汇体系，以及反-反政治的全新视野。

“顿悟”与实践的益处

目标在于引发顿悟 —— 即当问题的结构性根源突然与个人经历产生关联时的那一刻。

正是这种顿悟聚焦并转化了愤怒。

更深的理解反过来可能缓解心理压力，使人更容易以愤怒而非抑郁或焦虑作出回应。即便某些团体排斥治疗过程中的适应导向和自尊建设，仍可通过将其塑造成自助形式来吸引参与者。

由此形成的亲密团队侧重视角与分析而非行动。但必须清醒认识到：这种新认知必须转化为某种行动，否则终将沦为徒增挫败感的自我审视。

助益

该策略将从多方面助力实践：

- 首先，这些团体可成为潜在行动者的储备库；
- 其次，它们能为未来的反抗时刻预热人心；
- 第三，它们创造了改变所谓“公众舆论”的整体场域的潜力，从而为行动创造一个更容易的背景。

[image]

这些团体还将作为生命支持系统，提供一个从对当下的沉浸中抽身出来的空间，提供一种激进和异议概念的熟练运用能力，这是当今大多数人所缺乏的。

挑战和对策

焦虑感源于"市场"对我们的要求始终模糊不清，顺从的诉求与一套无法预先确立的模糊标准相连。如今，即便是最顺从的人，也会因管理或生产新技术的引入而被抛弃。小组讨论和意识提升的功能之一正是构建解读现状的视角。

核心挑战在于：如何在持续的时间与注意力压力下维持定期的投入。

这个过程的节奏较之当下文化所能接受的更为缓慢，尺度更具人性化。然而团体能提供日常斗争中的喘息之机，以及一种可能缓解注意力压力的更安静的互动和倾听方式，这也可能具有吸引力。

参与者需学会以自我表达的声调发言（而非源于分享琐碎信息的迫切需求所衍生的新自由主义表演！），并掌握倾听与分析的能力。

另一难题在于经验的复杂性。由于符号资本主义代码中内嵌的细微歧视，个人经验呈现强烈差异化，这使得分析环节尤为关键。

[image]

最重要的是，该过程应确立关于焦虑根源的新命题。这些命题可成为新型抗争形式、新战术的基石，并唤醒当前受压抑的行动力量 —— 这正是对抗焦虑的战斗机器。

[image]

后记：原因与情感

当我们将资本主义理解为情感性的 —— 即通过生产并依赖特定情感、态度及关系模式来维系自身 —— 诸多现象便豁然开朗。

这些情感并非单纯的经济关系产物，而是 构成关系本身的核心要素。

驱动经济的所谓物质需求实为社会建构，正如其要求的服从与疏离亦受文化塑造。现代劳动者和消费者的个人主义倾向、我们与万物的疏离感、将金融视为“实体”而将生态视为“抽象”的怪异认知，尤其是我们习以为常的私有财产与权威观念—— 只要剥离这些，看似永恒不可撼动的市场体系便会崩塌。

试图通过追踪股市而非立足生活经验来理解经济，恰恰暴露了资本主义赖以生存的根源性割裂。

私人情感与人际关系和物质条件同样根本。我们需要探讨情感状态的语言体系。

通过这种视角审视资本主义关系，能阐明诸多现象：例如抗议活动即便未能消除诉求对象的不公，参与者仍可能获得满足感 —— 有时甚至强于直接诉求被满足时的感受。我们珍视广场上共叙往事的夜晚，珍视坚守阵地的时刻，远胜于偶尔赢得的微薄让步。迄今为止，这种现象通常被轻率地归因于"捍卫尊严"的口号。但当我们将资本主义下的生存状态视为情感性存在时，便能理解为何那些改变情感状态的抗争形式本身就能带来满足感 —— 而非仅仅作为填饱肚子、调高暖气温度的手段。正如占领运动及其他抗争所揭示的：若能摆脱苦闷、厌倦与焦虑，许多人甘愿啃干馒头，睡在赤裸的砖地上！同样地，将我们面临的问题定位为情感问题，能帮助我们避免追求或接受那些无法改变我们感受与联结的表面解决方案。

[image]

究竟什么才能真正对抗焦虑？

我们是否必须在保安、保险政策、宗教团体和抗抑郁药物的游戏规则中胜出，以某种方式让人们在一个充满敌意和危险的世界中感到安

全？

试图将缓解焦虑作为一个独立于废除制造焦虑的条件之外的项目，就注定会失败。

我们是否该接受最坏情况已成定局，“加速”迎向它，将焦虑转化为武器？

如果焦虑是现行秩序无处不在的守护者，它恰是抵抗运动的绝佳切入点 —— 但这并没有解答：已被焦虑禁锢的人们如何完成这种炼金术？

或许在对抗统治秩序的过程中，我们能共同创造出激发信心的存在，立足于共享的现实认知—— 这种认知既非市场也非军队所能夺走。

BY 不确定意识研究所

[image]

【转评论 —— 2026/0325】

用这篇文章来理解 #张雪峰 及诸多华人中产阶级和社会网红，是非常贴切且重要的。

这是20年前北美激进派中一度超热的理论，它正确地指出：资本主义的每个阶段都存在其主导的反应性情感：19世纪是苦难，20世纪是无聊，而本世纪就是 - 焦虑。疯狂消费粉刷门面、无止境的斜杠追求装点人设、整容热、健身热、自拍热、各种昂贵的抗衰老智商税，用泛滥的成瘾物品伪装精气神儿 ...所有这一切只为能继续留在那台虚妄的跑步机上。

如您所见，这就是当前华人所经历的和普遍深刻感知的事实。你我就是这样被彻底控制住的。

原子化是这一控制系统的枢纽：真正的交流日益罕见、亲密关系凤毛麟角…

尤其是，此理论正确地强调：谁能真正解决焦虑问题，谁才是本时代成功的革命者。

张雪峰和很多中产阶级及社会网红都属于一定程度上的聪明人，他们意识到了“焦虑”这一主导情绪的巨大利益。然而同时他们却又无比愚蠢，他们意识不到问题的根源，看不清自己也深陷其中，以至于持续相信自己能从他人的困苦中汲取源源不断的利润。

我昨天说，张雪峰之死作为一个隐喻具有深刻意义。但是除非它能促进中产阶级对其自身尴尬立场的深刻反思，否则此意义将继续被埋没。

 https://m.cmx.im/@MitteKeegi_@mastodon.social/116288454778283263

[image]
[image]

运动创伤的处理和应对技巧：心理安全S08E06

[image] 关键词	互助 创伤 压力 心理安全 抵抗 自助
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月8日
[image] **Description**	心理安全

不要害怕创伤。即使一度被击垮，仍有可能在事后变得更强大、更睿智。健康的成长需要时间的积累，应对创伤亦是持续的过程。

- Table of Contents

潜在创伤事件发生前
潜在创伤事件发生时
创伤事件后
警惕余震或创伤后应激障碍的细微征兆。可能出现以下任一/或组合症状：
如果出现以下情况，患者可能需要进一步治疗：
重大创伤后数日/数周内，患者可能需要以下支持：
身体疗法资源
安顿练习
PROVE
DEARMAN
情绪管理
1、表达/释放情绪。这是最理想的方法！
2、容纳/压抑情绪
3、保护情绪
帮助他人应对心理创伤的STOP12345模型

创伤事件事后分析的七个阶段
第一阶段：介绍
第二阶段 —— 事实
第三阶段 —— 思考
第四阶段 —— 反应
第五阶段 —— 症状
第六阶段 —— 教学
第七阶段 —— 重新融入
推荐阅读

[image]

何为“创伤”？创伤是指任何超出个人或集体应对能力的经历。

不要害怕创伤。即使一度被击垮，仍有可能在事后变得更强大、更睿智。健康的成长需要时间的积累，应对创伤亦是持续的过程。

我们携手应对创伤，从而汇聚集体力量与社区凝聚力。

潜在创伤事件发生前

1. 指定支持人员：为整个团队或每位成员指定支持人员。

1. 向支持者告知创伤风险因素，例如：
   - 情绪障碍或人格障碍病史
   - 既往创伤经历
   - 静息心率高于正常值（＞95次/分钟）
   - 缺乏社会/家庭支持及资源

1. 预演：预演可能的情境，为潜在创伤结果制定"预案"。

1. 培养乐观态度：培养对生活、运动、行动的广泛乐观态度。

1. 叙述：人们通常需要“理顺思绪，让事情变得合理”。提前开始

这项工作。

1. 练习正念：正念有助于事后的恢复，但必须预先培养。

1. 可能的支持清单：让参与者列出支持他们的人和事物的清单，供后续参考。

潜在创伤事件发生时

1. 保持团队行动，结伴同行 —— 搭档制。

1. 设置专属"放松区"供休息。

1. 重申行动的叙事/意义和集体团结（“声援”/“团结”）。

1. 如果有人突发严重焦虑，请尝试：

- 引导其前往相对安全的地方。

- 如果对方回避眼神接触，询问"眼神交流是否能缓解"。

- 邀请对方与您一起呼吸：初期同步呼吸节奏，逐步放缓。

- 询问是否需要拥抱/肢体触碰。

- 用愉悦事物转移注意力：气味（橙皮、薰衣草、薄荷糖）可帮助回归现实世界。

- 询问令其平静的事物，请详细描述。

创伤事件后

- 给予倾诉空间，但切勿施压要求发言。
- 接纳情绪/寻求情绪认同。避免轻描淡写或拿"更糟糕的情况"作比较。
- 构建叙事框架。借助过往经历的启示，或设想事件对世界的深远意义，帮助当事人理顺思绪，"赋予事件意义"。
- “寻找帮助者”： 也许可以从讨论在事件中或事后有哪些帮助开始。团队可以从讨论在创伤发生时或刚发生后，谁或什么起到了保护或治愈作用，来开始事后分析。

警惕余震或创伤后应激障碍的细微征兆。可能出现以下任一/或组合症状：

- 噩梦
- 与情境不符的恐惧；或在危险情境中反而缺乏应有的恐惧感
- 止不住地思考那件事，或者完全无法思考
- 睡眠周期紊乱，睡眠过多或过少
- 食欲紊乱，暴食或忘记进食
- 莫名烦躁或愤怒
- 注意力涣散

- 社交行为改变，如害怕独处、或自我隔离

如果出现以下情况，患者可能需要进一步治疗：

- 主动寻求治疗
- 症状随时间推移持续恶化
- 症状持续数周以上影响正常生活

重大创伤后数日/数周内，患者可能需要以下支持：

- 提醒进食或提供食物
- 提醒更换干净衣物，协助洗衣
- 提醒其他自我护理事项：如沐浴、服药、饮水
- 提供倾诉机会，或无需谈论创伤的社交空间
- 通过体育锻炼释放积压的紧张情绪
- 多种形式的身体接触，从拥抱到跆拳道皆可（需征得同意）

具有镇静功效的草本、补充剂或茶饮（如果正在服药或存在健康问题，使用草本或补充剂前务必咨询医疗专业人士）。

推荐选项包括：

- 洋甘菊

- 西番莲
- 薄荷
- 柠檬香蜂草
- 薰衣草
- 卡瓦（肝功能异常者禁用）
- 镁补充剂（临床低血压者禁用）

身体疗法资源

- 针灸/指压疗法（尤推荐NADA耳穴疗法）
- 按摩（泰式按摩效果显著）
- 瑜伽

[image]

安顿练习

安顿练习不仅对遭遇强烈情绪或创伤反应的队友至关重要，更是每位队员都应掌握的自救工具。这不是很容易做到，难免会产生自身的情绪反应。

许多人拥有适合自己的技巧，请务必引导他们识别并运用这些有效方法。

以下是一些安顿练习的简要方法清单：

- **54321**：

说出5件你看到的事物、4件你听到的声音、3件你能触摸的物品、2种你能闻到的气味，以及1种你能品尝的味道。

- 节奏呼吸法：

这种呼吸技巧要求呼气时间长于吸气，例如吸气计数3，呼气计数4。

- 借助物品：

握住某物，观察并描述其特征。钥匙扣是理想选择 —— 它拥有不同质地、色彩，摇动时还能发出声响。

- 计数练习：

从100开始倒数，每次减7（或任何需要稍加思考的数字都可以）。

- 调整身体姿势：

看似简单，但移动身体能帮助我们锚定当下。

- 字母游戏：

设定类别，按字母顺序列举该类别的物品。此法亦适用于团体练习。

- 运用气味（如精油、橙子、薄荷糖等）：

嗅觉常是人类最敏锐的感官输入之一，能有效帮助人们回归当下。

我们鼓励人们制作随身携带的"应对卡"，一侧记录支持性资源，另一侧简要列出个人有效的应对技巧。因为当情绪高度痛苦时，人们经常难以回忆有效的应对方法，这张卡片就可以成为危机/高压时刻可供参考的具体工具。如果您是协助者，可询问对方是否需要协助运用卡片上的技巧。

PROVE

彻底开放型辩证行为疗法（RO-DBT）教授名为PROVE的技巧，旨在培养开放心态下的坚定表达。如需采用框架模型，这一方法可作为设定边界的参考范式。

1. 简要描述情境
   —— 客观陈述导致你接受/拒绝请求的背景，避免辩解、辩护或合理化 —— 例如："我注意到你频繁联系我寻求高强度支持。"
   —— 使用限定词来表达开放态度和谦逊，为可能的误判留出空间，例如："据我观察……""我不确定是否正确，但似乎……""有没有可能……？"

1. 表达情绪时避免指责
   —— 坦率直接地表达你的情绪，避免将其视为事实陈述。使用"我"开头的表述。
   —— 例如："当你频繁联系我寻求支持时，我担心自己无法持续提供你所需的帮助。我意识到自己产生了'你可能没有其他倾诉对象'的想法，这引发了我的忧虑，因为我并非总能成为你的主要依靠。"

1. （承认）对方的需求。
   —— 让对方知道你愿意考虑他们的想法和感受；
   —— 不要断定自己完全了解对方的内心想法、感受或意图；
   —— 询问对方除了你个人的帮助之外还需要其他什么（例如：他们是否需要帮助寻找其他支持资源？你能否协助他们获取更多资源，从而减少对你的依赖？）；

—— 例如："对我来说，能够提出我的需求并了解你内心的体验，即使它与我的想象不同，也会让我觉得我们都很珍视这段关系。"

1. （运用你重视的目标）来指导你如何通过社交方式表达你的需求。
—— 例如，采用非支配性的开放姿态，允许事情不必立即得到解决；
—— 应以冷静克制的方式回应，避免使用间接的断言和伪装的要求，更不要诉诸于人；
—— 保持礼貌，尤其考虑到此类讨论可能较为敏感。例如："我想和你确认这件事并请你帮忙。能否请你减少联系我寻求支持的频率？"
—— 如果情况对你造成强烈的负面影响，或者你的需求至关重要，请传递紧迫感并重复请求，同时通过挺直的腰身、保持眼神接触等动作展现自信。切勿吼叫也不要耳语。

1. 基于自我照护来判断是否需要重复表达或加强表达力度
—— 以您期望的关系亲密度为基准，调整表达强度。如果满足自身需求至关重要，请持续表达直至需求得到满足。
—— 如果对方质疑、反驳或忽视您的主张，切勿立即回应。先自问能否从该情境中汲取经验，再作回应。
—— 如果这是您希望维系的亲密关系，切勿过度索求。在亲密关系中反复强调同一事项易被视为胁迫。不妨请求对方协助化解僵局。

DEARMAN

辩证行为疗法（DBT）提供名为DEARMAN的技巧，用于人际场合达成目标。这也是可用来设定边界的实用模型：

1. 描述情境时不做评判，例如：

- "我告诉过你我不想去酒吧，可你一直试图说服我应该去。"

1. 表达自己的感受：努力在表达自我与保持自制之间找到恰到好处的平衡点。

- 在每一次表露前问自己：“现在以这种方式表达，我将来会喜欢自己的感觉吗？”

1. 坚定立场

- 避免被动和攻击性（也包括避免被动攻击）。

1. 强调积极结果

- 提醒自己和对方尊重你的请求的积极结果。

1. 正念

- 练习全然接纳、反向行动和正念呼吸。当你感到犹豫、压力过大或可能屈服于侵犯边界的压力时，运用这些技巧。

1. 展现自信

- 通过自我肯定来强化信念：你的边界是合理的。即使心存疑虑，也要努力保持冷静自信的姿态。

1. 协商

- 预先确定可接受与不可接受的妥协范围

- 在内心确立边界，并明确界定边界被侵犯或妥协时将面临的后果

- 预判哪些让步你能接受，哪些可能令你后悔。

情绪管理

面对情绪时我们有三种选择，但每个人差异巨大，选择不同选项的临界点也各不相同：

1. 表达/释放情绪

1. 容纳/压抑情绪

1. 保护情绪

接下来，我们将深入探讨这些选项。

1、表达/释放情绪。这是最理想的方法！

你清楚自己正经历这些情绪，但未必需要明确它们的具体内容。那该如何操作呢？

- 向安全且善解人意的人倾诉是表达情绪的好方式，但这至少需要对情绪本身有基本认知。

- 哭泣是身体释放情绪的自然途径 —— 放心哭吧，没关系！

- 肢体活动能帮助释放那些难以言喻的情绪 —— 否则情感会滞留在身体里。

- 创作（如艺术、写作、手工艺、建造等）有助释放未知情绪，拓展你描述它们的方式。

2、容纳/压抑情绪

当你需要专注处理当务之急时，这很有效，但并非长久之计。

终究需要表达/释放出来。

有时他人能通过拥抱提供帮助。别忘了要先征得同意。

3、保护情绪

当情绪汹涌时，人们常通过攻击他人来保护自己，但这只会制造更多待处理的情绪。

有时又会通过压抑隔离来保护自己的感受。

这两种方式都效果有限 —— 情绪往往相互滋养。因此，理想状态是找到表达途径！

帮助他人应对心理创伤的STOP12345模型

1. 「该不该帮忙、怎么帮」

我该直接帮助此人吗，还是帮TA寻找其他帮助？

对于这个问题，请首先考虑您自身的身心舒适度，是否需要对方稍后再来找您，以及需要哪些条件才能最有效地提供帮助。

1. 「你现在怎么样？」

提出开放式的、不带评判的问题，切勿追问创伤细节。

只需掌握大致情况。

注意自身承受细节的限度并严格遵守，但对话细节程度应由对方主导。

如果对方情绪过激或者出现精神抽离，请将话题拉回当下。

1. 隔离情绪避免感染

维护并执行你的心理界限。在对方的感受和你自己的感受之间保持分离（例如，不要承担别人的情绪体验）。因为这样既没有用还有害。

时刻关注您自身内在的感受，如果感到不堪重负，请回到第一条原则。

1. 「还有其他情况吗」

是否存在加剧当前问题的其他心理或生理状况？是否还有其他面临相同困境的人需要类似帮助，或能相互支持？

1. 实施干预

当您厘清状况后，就可以开始介入了。

可询问对方是否需要倾诉，或是否希望获得解决困境的实际帮助。

可询问是否需要某种舒缓的接触，或者主动提供食物、饮水、保暖衣物等物质支持。

当干预措施完成或对方不再需要即时的支持时，制定具体的后续跟进计划。

最简单的表达是"明天发消息问候你近况"。如果无法亲自跟进，可承诺 "几天后安排小组成员探访"。

您也可以询问对方是否有希望联系的朋友或支持者。

您的后续行动只需确认对方已联系到其他支持资源即可。

创伤事件事后分析的七个阶段

第一阶段：介绍

向小组提供以下信息：

- 事后分析期间的所有陈述、事实、观点及讨论均须严格保密。
- 禁止录音或记录笔记。
- 不得因个人感受而批评任何人。应允许成员自由表达情感，彼此间需给予接纳、支持和理解。
- 会议开始后成员不得离场。
- 所有成员均须参与第一阶段讨论，后续阶段可自主选择参与。
- 事后分析绝非对关键事件中团队行动的批判。
- 重要提示：严禁媒体参与！

第二阶段 —— 事实

向参与者提问（回应可选）：

- 请做自我介绍。
- 事件中您扮演了什么角色？
- 请用客观事实描述关键事件。

重要提示：此类提问适用于20人以下的小组，要求每位成员回答相同问题。

若小组规模较大，可采用不同的方法（遵循时间顺序：事件发生时：谁最先抵达？谁随后抵达？发生了什么？）。

第三阶段 —— 思考

参与者被问及（回应可选）：

- 当您摆脱下意识的行动后，对事件的最初想法是什么？

重要提示：此阶段使参与者将经历内化为个人体验，使其成为自身的一部分，而非置身事外。

第四阶段 —— 反应

参与者被问及（回应可选）：

- 对您个人而言，事件中最糟糕的部分是什么？

重要提示：本环节时长约30-45分钟（视事件强度而定），重点关注参与者的情绪状态。

第五阶段 —— 症状

参与者被问及（回答可选）：

- 当前可能出现的心理困扰征兆和症状有哪些？

重要提示：通常会讨论三类症状出现的时段：

- 事件发生时的即时反应；
- 事件发生后数日内的持续反应；
- 以及事件3-5天后仍残留的遗留反应。

第六阶段 —— 教学

- 向所有参与者提供减轻家庭、工作等场景压力的实用信息。

第七阶段 —— 重新融入

- 引导小组成员提出他们可能有的任何问题。
- 小组可重新审视事件中仍令人不安的部分。

- 成员甚至可能提出先前未讨论到的新问题。

重要提示：本阶段小组负责人可提供鼓励与支持，并引导成员思考此次事件中可能产生的积极意义。建议为每位成员准备资源清单（含电话号码及地址）。

免责声明：事后讨论是帮助人们处理创伤事件直接经历的重要第一步，但咨询师必须接受过专门培训，方可开展任何形式的幸存者事后讨论活动。

推荐阅读

- Aftershock: Confronting Trauma in a Violent World: A Guide for Activists and Their Allies" by Pattrice Jones

- "Critical Incident Stress Debriefing: CISD : An Operations Manual for the Prevention of Traumatic Stress Among Emergency and Disaster Workers" by Jeffrey T. Mitchell

- "Trauma Stewardship: An Everyday Guide to Caring for Self While Caring for Others" by Laura Van Dernoot Lipsky and Con- nie Burk

- "Trauma is Really Strange" by Steve Haines (Author) and Sophie Standing (Illustrator)

[image]
[image]

“没有未来”的未来：沮丧，左派和心理健康的政治 - 心理安全 S08E07

[image] 关键词	个人 关系结构 抑郁症 治愈 集体革命
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年4月30日
[image] **Description**	心理安全

> 我们发现，在资本主义那套"行不行都得行"的残酷循环机制下，我们竟连尝试的勇气都丧失殆尽了 —— 纵使内心渴望挣脱，然终究在病痛、抑郁与麻木中自我禁锢。 —— 安妮·博耶《失望命运手册》

[image]

“如果你连床都爬不起来，还怎么上街起义？” 乔安娜·赫德瓦在《病弱女性理论》中提出的这个问题，在我心头萦绕许久挥之不去。为何？因为它指向我们中许多人都深谙的境况：一种绝望和抑郁交织的困境。一种你真的无法下床的境况。

这种境况在多数情况下，还浸透着政治与经济的影响。

与主流心理和精神医学话语相反，你“无法下床”的原因并非源于所谓的消极态度、负面思维，也并非是你“主动”选择了不幸；更非单纯的生化失衡 —— 无论是脑内化学物质紊乱、不幸的遗传倾向，还是血清素水平低下。更多时候，根源在于你身处的世界：那份令你厌恶的

工作，或是刚刚失去的职位；来自未来的债务如幽灵般侵蚀当下；以及这个加速滑向深渊的世界。

[image]

本文基于一篇博士论文及个人经历 —— 我曾在2013/2014年经历过抑郁问题 —— 试图探讨抑郁症与政治的关系，思考当下时代的政治经济与心理病理学的关联。其立论根基在于一个事实、一项主张、和一次呼吁。

首先是事实：正如丹麦心理健康基金会所揭示的，该国抑郁症确诊人数持续攀升。任何时刻都有4%至5%的人口处于抑郁状态，或更准确地说，被确诊为抑郁症。丹麦卫生管理局数据显示，2011年超过45万丹麦人购买抗抑郁药物，这一数字在过去十年间几乎翻倍。此类趋势在整个西方世界均有体现。美国国家心理健康研究所估计，7.1%的美国成年人口（1730万人）正遭受抑郁症困扰。另有数据显示，每五名美国人中就有一人受抑郁症影响。这些数字促使世界卫生组织得出结论：抑郁症是最常见的精神障碍，也是导致残疾和自杀的首要原因，全球约3.5亿人深受其害。因此，全球选择性血清素再摄取抑制剂（SSRI类抗抑郁药）的消费量激增也就不足为奇了。据市场研究公司 alliedmarketresearch.com 的数据显示，该类药物年销售额现已逼近**140**亿美元。该公司还以相当笨拙的措辞指出："导致抑郁症的因素众多，包括基因、压力及脑部化学物质等。”

其次是主张：抑郁症以最极端病态的形式，昭示了当代主体的异化。因此，这种精神病理必须与资本主义现实主义的世界相关联 —— 正如撒切尔得意洋洋宣称的那样，这个世界确实“别无选择”，未来似乎已永远冻结。抑郁症恰好就成为了历史性资本主义未来危机的症候。正如雷蒙德·威廉姆斯所言，它是一种情感结构。因此，任何抑郁症的疗法都必须采取集体性、政治性的形式的；与其将精神疾病问题个体化，不如开始质疑将精神心理问题个体化的现象本身。

[image]

正因如此，左翼必须严肃对待疾病和精神心理障碍问题。应对抑郁症及其他精神病理现象，不仅是当代解放事业的组成部分，更是其可能性的前提。在我们能够砸碎窗户之前，必须先学会从床上爬起来。

[image]

抑郁症领域最杰出的政治思想家仍是已故的马克·费舍尔，他终生饱受抑郁症折磨，最终因病自尽。其全部著作都在持续探讨抑郁症作为个人体验与社会政治体验的双重维度。

在2009年出版的《资本主义现实主义》一书中，他将抑郁症与我此前所提到的"资本主义现实主义"相联系 —— 即"普遍认为资本主义不仅是唯一可行的政治经济体系，甚至已无法想象任何连贯的替代方案"的认知。在这部著作中，抑郁症成为资本主义现实主义运作机制的典型范例，是我们受阻且黯淡的历史处境的一个症状。

在2011年发表、后收录于2018年出版的《K-Punk：马克·费舍尔文集与未刊稿（2004-2016）》中的《压力的私有化》一文中，费希尔指出悲伤与抑郁的区别在于："悲伤自认是偶然且暂时的状态，而抑郁却呈现为必然性且永无止境的境况：在抑郁者的世界里冰川延伸至所有可想象的地平线。" 正因抑郁具有这种特殊属性，"抑郁者看似'现实主义'的极度降低预期，与资本主义现实主义之间存在着奇异的共鸣。"

而在2014年的《一无是处》一文中，费舍尔坦言自己的抑郁症始终伴随着一种根深蒂固的信念 —— 他确确实实"一无是处"。他写道，曝光自己精神痛苦的经历并非认为其有多特殊和独特，而是"为了佐证这样一种主张，即认为：许多抑郁症形态最适宜通过非个人化的、政治化的框架而非个人化的、'心理学化'的框架来理解 —— 并加以对抗。"

[image]

对抑郁症达成一种政治性理解的重要性再怎么强调都不为过。如果读者只能从本文领悟一件事，请务必记住：抑郁症存在超越任何诊断手册的成因与具体语境，更超越了新自由主义意识形态 —— 后者执着于主体而非结构、个人责任而非集体责任、化学反应而非资本。

然而，通过政治框架来理解抑郁症，并不意味着抑郁症问题能立即通过政治手段得以解决。抑郁症蕴含着一种恐怖，无论我们怀有怎样的批判性与革命性愿望，都不能也不应将其过快地转化为政治议题。任何经历过抑郁 —— 或身边有人抑郁 —— 的人都深知，那简直是人间地狱。肉体痛苦令人窒息，身体沉重如铅，心智几乎完全停顿，你无法摆脱那种被困住、停滞不前的感觉，仿佛比赛已然结束，而当下 —— 这地狱般的现实 —— 既是全部，亦是未来唯一可想象的存在。

如果轻描淡写地说，“这只是政治问题”，实属冒犯。同样地，我们也绝不该美化所谓的"抑郁现实主义"，因为这种"现实主义"不过是资本主义现实的附庸：宣称别无选择，宣称对现状束手无策。这是我们必须认清的另一重真相。更不可忽视的是抑郁症是自杀死亡的主要诱因—— 据世卫组织最新报告，全球每年自杀人数接近80万。

第三点也是最后一点在于：书写抑郁症确实困难重重。此处所指不仅是书写自身抑郁的艰辛，更在于如何在描绘巨大痛苦的同时，既能确立自身立场，又能构建不致令人彻底绝望的抑郁症话语体系 ——尤其在马克·费舍尔不幸离世之后，这种困境尤为沉重。

[image]

关于抑郁症，我们掌握大量事实，但这些事实本身并不能说明问题。抗抑郁药的销售量并不完全对应抑郁症的发病率，因为选择性血清素再摄取抑制剂（SSRIs）不仅用于治疗抑郁症，还用于治疗多种其他精神疾病。诊断频率未必反映抑郁症的实际发生率，因此诊断数量的增长既可能表明抑郁人群增多，也可能反映出一种日益严重的病理化倾向 —— 即将悲伤等常见的"正常"情绪转化为抑郁症的诊断范畴（最新例证是《精神疾病诊断与统计手册》和《国际疾病分类》等新版诊断手册将悲恸也纳入到抑郁症范畴）。

我们还需思考：为何精神病诊断似乎能带来如此大的慰藉？因为抑郁症的诊断本身具有抚慰作用。原来这就是我感觉如此糟糕的原因！抑郁症！大脑化学物质失衡！这种诊断为无意义的痛苦赋予了短暂的意义。痛苦有了名称和成因：血清素缺乏。但这个成因本身另有根源—— 在诊断体系中，乃至整个资本主义世界里，这些根源始终没有被诊断也未被揭示。

正如马克·费舍尔在《资本主义现实主义》中所写道的：

毋庸置疑，所有精神疾病都具有神经学上的体现，但这并不能解释其成因。例如，如果抑郁症确由血清素水平低下引发，仍需阐明为何特定个体存在血清素缺乏。这需要社会政治层面的解释；如果左翼欲挑战资本主义现实主义，重塑精神疾病的政治属性便刻不容缓。

但在探讨抑郁症成因之前，且容我先描述下围绕抑郁症的道德话语。

以莱奥·古拉制作的自助视频《我为何抑郁》为例。根据其推特简介，这位"专业自我提升爱好者、生活教练人生导师、视频博主、企业家兼演讲者"致力于"帮助人们设计精彩人生"。

古拉，这位留着山羊胡的光头男子，同时也是 actualized.org网站的创始人，在视频开头表示他想解答标题提出的问题："为什么我 —— 你[挑眉，同时双手在空中比划出括号状的手势，仿佛将这个词括起来] —— 会抑郁？" 他给的答案很简单：你抑郁是因为你的心理状态糟透了。值得注意的是，这恰恰是艺术家组合克莱尔·方丹某部视频作品的标题 —— 他们在2015年创作的现成品视频《无题（为何你的心理状态糟糕透顶）》中，一位非裔美国女演员几乎逐字复述了古拉的演讲，对新自由主义自助产业将抑郁症意识形态化、将主体普遍责任化的现象展开了尖锐而滑稽的批判。克莱尔·方丹是艺术界最专注且持续探讨抑郁症议题的创作者之一。在他们的创作中，抑郁始终具有政治属性，必须结合其真实根源 —— 资本主义债务经济与金融投机体系中的社会冲突 —— 来理解。

回到原始视频，古拉的开场白之后，一连串闪烁的标语或关键词依次出现。按呈现顺序，这些词语是："成功、幸福、自我实现、人生目标、动力、生产力、巅峰表现、创造性表达、财务自由、情商、积极心理学、意识、巅峰表现、个人力量、智慧"。（显然"巅峰表现"这个概念被认为至关重要，以至于必须重复强调。）随后古拉抛出核心观点，声称揭示惊人真相："实话告诉你，说白了你抑郁的根源就是心理素质太差了。没错，你的心理状态一团糟，你丫情绪不稳定！我不是在责备你，只是陈述事实。" 他随即澄清，此处并非指"临床抑郁症"患者 —— 那些确诊为"真正抑郁症"的人群。他所指的是我们这些多数人——尽管他声称自己没有指责，但他确实是在指责。这段视频时长略超20分钟，其中莱奥·古拉直言不讳地宣称："你的抑郁就是你自己造成的。" 你的心理认知机制出了问题，你的心理素质就是"垃圾"。别当受害者了，掌控自己的心理状态！追求巅峰表现！

嘲笑这段视频并调侃其逻辑固然容易，但这种逻辑在当今世界占据主导地位 —— 即便有时以更温和的方式表达 —— 且具有实际影响。其核心逻辑是：人创造自己的现实。单凭思想就能改变事物。这意味着你亲手编织命运之线，"不存在"外部环境，更无任何借口可言。

一位名字带有准皇家色彩的丹麦社会学家艾米莉亚·范·豪恩在其主页上表达了相同的逻辑："幸福是一种选择 —— 你的选择"。同为丹麦人的治疗师伊娃·克里斯滕森也对此深表认同，她说：「幸福是个人责任。幸福不是你能指望从他人那里获得的东西。每个人都握有通往自身幸福的钥匙，因此也肩负着将钥匙插入正确锁孔的责任。幸福源于内心，让他人使我们幸福并非他们的责任，而是我们自己的责任。正如我们无法改变他人，只能改变自己。」

如果个人要为自己的幸福负责，那么TA也必须为自己的不幸负责。既然“钥匙掌握在自己手里”，我们每个人几乎都要为所有事情承担个人责任。成败与否，健康与否，全凭主观意志、生活方式和个人选择决定。虽然我们或许无法改变他人，甚至无法改变世界，但我们完全能够努力改变自己。结构性变革 —— 即制度变革 —— 就这样被摒弃了，取而代之的是主观性变革 —— 自我改造。无论社会、政治或经济层面的任何问题，皆被个人化甚至罪恶化：主体被要求为自身不幸负责，既要独自承受痛苦，又要因感到不快乐、未能成为“优秀公民”、拒绝上班、赖床不起而背负罪责。

所谓的积极心理学与幸福至上主义所蕴含的个人化和责任化的这些过程是相辅相成的。马克·费舍尔敏锐洞察了这种逻辑，或者说意识形态。抑郁者被不断灌输这样的观念：他们的抑郁完全是自身过错。"个体宁可自责也不愿归咎社会结构 —— 毕竟他们已被诱导相信社会结构根本不存在。"他在《无用之人》中如此写道，此处暗指撒切尔夫人另一句名言："社会并不存在"。

抑郁症问题由此延伸为更普遍的困境：利奥·古拉在原始自助视频中倡导的主体性模型，与资本主义主体性的虚构 —— 即自主、自我决定、竞争性个体模型 —— 完全一致。在视频中，"观众" —— 即"你" —— 既是抑郁的根源，亦是唯一的解药。视频旨在教你如何"掌控心理"，最终将你带入"全然的幸福与喜悦"之境。

这传递着深刻的道德论调：无法获得幸福即是不道德。如果你沦为如此不道德的糟糕之人以致陷入不快乐 —— 或抑郁 —— 那责任全在你自己身上。这正是当代资本主义的归咎教条：你正在制造自己的抑郁 —— 即便事实显然并非如此。

[image]

换言之，资本主义对抑郁症患者造成双重伤害。

- 首先，它引发或加剧了抑郁状态；
- 其次，它抹去任何形式的因果关系，将疾病个体化，使抑郁症看似个人问题（或个人财产）。

某些情况下，它甚至被归咎于患者自身。倘若你曾活得更充实积极，做出不同选择，保持更乐观的心态等等，便不会陷入抑郁。这正是全球心理学家、教练和治疗师们反复唱响的调子：幸福是你的选择，你的责任。不幸与抑郁亦复如是。资本主义先让我们感到痛苦，继而雪上加霜地让我们自己去为这种痛苦感到愧疚。

基于我自身抑郁症的经历 —— 尽管这并非真正意义上的"个人经历" —— 以及就此主题撰写的博士论文，我认为毋庸置疑：我们需要对抑郁症进行新的分析，同时也需要另一种疗法。

面对抑郁症的个人化倾向，必须以抑郁症的政治化来回应。

在分析层面与社会成因层面，抑郁现象都应与劳动、工作及失业问题挂钩 —— 统计数据显示，失业者比在职者更易陷入抑郁，无论这些有工作的人多么讨厌自己的工作。抑郁症还应与残酷的新自由主义竞争文化（“饥饿游戏快乐，愿好运永远伴随你！”）及伴生的幸福意识形态挂钩 —— 这种意识形态强迫人们永葆笑容、时刻快乐，即便正在彼此厮杀、为生计挣扎、勉强度日之时，亦不例外。抑郁症更应与教育领域挂钩：在我任教的哥本哈根大学，众多学生饱受各类精神疾病困扰的现象已昭然若揭。我甚至不敢想象英国或美国的情况 —— 那里学生不像丹麦这样享有免费教育，反而被越推越深地卷入债务漩涡。无论目光投向何处，学生们都深陷抑郁、焦虑、压力与精疲力竭的泥沼。

经济危机爆发后，大量研究开始关注债务对心理健康的影响。2012年，经济学家约翰·盖瑟古德发表的研究表明，深陷债务泥潭的人群普遍存在抑郁等多种心理问题。所有证据都表明，负债不仅会增加抑郁风险，更会显著提升自杀倾向。另一项研究发现，"在控制社会人口

学、经济、社会及生活方式等因素后，负债者产生自杀念头的概率仍高出两倍"。而在《经济之躯：紧缩政策为何致命》一书中，大卫·史塔克勒和桑杰·巴苏通过流行病学研究揭示：相较于经济衰退本身，紧缩政策对公共与私人健康状况造成的破坏性影响更为严重。书中提及一项针对50岁以上美国人的研究发现："2006至2008年间，房贷拖欠者出现抑郁症状的概率高出约九倍"。他们得出令人沮丧的结论：紧缩政策不仅造成伤害，更会夺人性命。希腊老人迪米特里斯·克里斯托拉斯的悲剧便是明证——2012年4月4日，他在希腊议会大厦前"将枪抵住头部宣告：'这不是自杀，是他们杀了我。'随后扣动了扳机。”

这些状况真实存在，其因果关联同样真实。显然，成因众多且复杂。但抑郁的症状也映射着其他问题的症结。事实是，债务经济体系正引发深重痛苦——负债者（无论是学生还是其他群体）被迫典当自己的未来。然而精神病学界与公共话语仍执意将抑郁症视为脱离背景的个人问题。这种倾向在诊断手册的论述中尤为明显 —— 这种话语正日益主导公众认知 —— 其中精神疾病仅被视为症状集合，完全忽视患者所处的历史、社会与经济背景。

因此，左翼对当下现实的分析不仅要坚持强调背景因素，更要与赫德瓦共同主张："正是这个世界本身使我们生病并持续折磨着我们。" 这里的世界并非抽象概念，而是我们身处其中、艰难跋涉的具体资本主义世界。这正是我们中许多人卧床不起辗转反侧的原因。正如酷儿理论家安·茨维特科维奇在其著作《抑郁症：一种公共情绪》中所论述的：

> 抑郁症的流行现象既可视为长期暴力历史的症状，亦可被其掩盖 —— 这种暴力历史在日常情感体验层面持续产生影响。[...] 在家庭领域被称为抑郁症的，正是这些社会问题的情感表征之一，它常使人陷入沉默、疲惫与麻木，以致于无法真正察觉自身不幸的根源（即便勉强察觉，也往往处于低水平的慢性悲伤状态 —— 或另一种抑郁形态）。

抑郁症的历史即是当代资本主义世界的历史 —— 用茨维特科维奇的话说，亦是暴力的历史：有色人种、LGBT群体或寻求庇护者每天所承受的暴力，既是肉体上的，也是精神上的。相关数据再次令人震撼，仅举数例：据索菲·刘易斯《全面代孕》指出，"38%的低收入母

亲及有色人种母亲会患上产后抑郁症"； 半数LGBT群体在过去一年经历抑郁；在丹麦的收容被拒庇护申请者的监狱式营地"舍尔斯马克出境中心"里，61%的儿童符合精神病学诊断标准。在诸多案例中，抑郁症正是这种暴力与脆弱性的印记，更令人痛心的是，它并非唯一的心理健康危机。

[image]

目前为止我尚未提及气候危机，但根据此前所述证据，生态与心理健康之间存在着密切关联 —— 此言绝非危言耸听。这并非忽视物质现实，而是暗示生态损失与全球变暖对心理造成的深远影响。

再次值得提及的是当今被称为"被毁掉的一代"的年轻群体（菲尔·尼尔在其杰作《腹地》中称其为"没有未来者大游行中的第一代"）。他们生活在一个明天很可能比今天更糟的世界，一个真正没有选择余地、没有未来可言的世界 ——气候危机正以最直观的方式摧毁着未来本身。谁又能怪他们抑郁呢？

这一切都在说明，当前的社会、政治、经济、生态危机，本质上也都是精神健康危机。资本主义永动机式的运转及其对资源的榨取，同样消耗着精神资源。经济与心理似乎已难以区分，正如"抑郁"一词的双重含义所暗示的。当然，我们并非同舟共济，亦非同病相怜。我们并非全都陷入抑郁（而那些抑郁者也未必以相同方式或因相同缘由承受痛苦）。我们遭遇的困境程度各异。某些社会阶层能以他人无法企及的方式触及未来，某些群体承受着更沉重的负担，某些人则比他人更早消逝。欧元危机中的希腊民众，或美国高等教育体系中的学生，其负债与抑郁的形态截然不同。如前所述，暴力与社会苦难沿着阶级、性别与种族的维度差异化分布；气候危机亦然 —— 哥本哈根的市民感受到的破坏性压力不如吉大港的居民。

坚持探讨疾病、心理健康与抑郁症的政治性时，必须时刻铭记这些地域性与全球性的差异。然而这不应演变为社会痛苦的竞争（“我最惨”） —— 竞争恰恰是资本主义的本质所在，它不断加剧这种竞争，使我们在承受痛苦的同时，又在彼此的痛苦中相互争斗。但这应当促使我们认识到：批判资本主义必须兼顾抑郁症及其他精神疾病的语境化心理病理学。更重要的是，它让我们窥见可能的"疗愈"路径 —— 我们需要做什么，如何从床上爬起来/走出困境（抑或，为何我们渴望走出困境）。

[image]

首先需要注意的是，对抑郁症及其背景的充分诊断本身并不足够。然而众所周知，诊断并不必然意味着治愈。仅仅知道问题所在，并不意味着我们就能解决它。相反，抑郁症的主要症状之一在于：你需要做的事情恰恰是你无法做到的事情 —— 至少无法独自做到。正如安·茨维特科维奇直白所言："指出资本主义（或殖民主义、种族主义）是症结所在，并不能帮我有力气从床上爬起来。"同样，我们没有理由相信废除私有制或实现全球性债务彻底清零就能像施展魔法般瞬间缓解抑郁者的痛苦。然而，在某种思辨中，我忍不住想说：革命是世上最有效的抗抑郁剂，它能创造更美好的世界，带来真正的幸福。但唉！要进行革命，我们必须先爬出被窝。这正是抑郁症的辩证悖论——真正的两难困境。

[image]

那么，关于抑郁症的政治学，或许一个好的切入点是：将痛苦集体化，将责任外部化，将关怀共同化。此时，责任问题再次以其全部的力度凸显出来。

必须拒绝新自由主义对抑郁主体的责任化要求，同时以集体责任的理念取而代之。

任何治疗项目亦应如此。

意大利思想家弗兰科·“比弗”·贝拉尔迪 —— 尽管他在临床术语的精准性上确实略显随意 —— 或许说得对："未来政治与治疗将合而为一。"治疗应是抵抗，而非对既定秩序的反动式服从；治疗应是集体工程，而非个体行为。治疗即是超越异化的过程。

这种集体性的解放性“疗法”可能呈现何种形态？我们拥有一个涵盖女性主义与艺术实践的档案库，其中收录了从奥德丽·洛德到克莱尔·方丹，乃至近期丹麦艺术家兼活动家雅各布·雅各布森的艺术关怀、自我关怀与集体关怀项目 —— 后者在经历严重抑郁症及数月住院治疗后，创立了“自我治疗医院”。我们需要一种语言，既能将这份档案汇入运动洪流，又能将其与制度化精神病学、新自由主义疗法及资本主义的利润追逐割裂开来。这种关怀超越了医院、诊所、家庭、国家、

保险公司乃至资本本身（即便一个人根本无法接触这些机构）。这种关怀基于对精神疾病的政治化理解，超越了商品化与资本主义形态的关怀。当身体相互照拂，当责任重新分配，当个体崩溃转化为集体亲密，未来便能以互助、共享与可持续之名被（重新）构筑。

这或许是构想抑郁症"疗法"的一种方式，既不强化顺从也不固守现状。可以肯定的是，任何名副其实的左翼政治都必须超越"资本主义是问题根源"的论断（尽管它确实如此），直面如何从床上爬起来的问题。这个命题既充满现实性，又具有革命性。当然，有时躺平本身就是一种革命行为，一种罢工，在日益围绕着强调积极肯定的"我能"运转的世界里，它化身为精疲力竭的消极否定——"不，我不能"。但总有人在探索新的起床之道：我仅顺带提及一个鼓舞人心的迹象 —— 资本主义现实主义的宏大建筑已现裂痕，可惜马克·费舍尔未能亲眼见证这一刻。

无论如何，重点显然不是摆脱抑郁以便重返最初导致抑郁的工作岗位。重点必须在于摧毁使我们生病的物质条件 —— 摧毁人们生活的资本主义制度，摧毁那些致命的不平等。由此，我们共同创造另一个世界。但要实现这一目标，要让这种可能性成为现实，需要的不是病患间的相互竞争，而是建立关怀联盟，让人们不再感到孤立无援，不再为自身病痛背负道德负担。通过彼此结盟，人们终将能够有力气爬起来上街战斗。

改编自《Going Nowhere, Slow》一书，Zero Books出版社，2019年11月29日出版。

[image]
[image]

“你若盛开蝴蝶自来”、“谁痛苦谁改变”、“接受你永远不会被爱的事实”... 自助文化的愚蠢流行及其威权主义本质 - 心理安全S08E08

[image] 关键词	威权主义 婚恋 性别 成功学 新自由主义 极化 法西斯 田园女权 红丸 自助励志
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵 ；
[image] 创建时间	2025年5月1日
[image] **Description**	心理安全

你觉得那些SBTI、MBTI的人格测试为什么能如此红火，一经推出瞬间刷屏？难道如今的人们都对自己的内心一无所知？不是的。测试本身并不是目的，目的是得到一个“权威”描述作为标识，以便呈现给周围人“看到”。这背后的驱动力是长期被忽视的哀伤、被误解的郁闷、被疏离的焦虑、被追赶碾压的恐惧、亲密无能的受害感。这些情绪真实且深刻。然而其被抓取和利用的方式比其本身更为可怕……

人们嘲笑着田园女权的愚蠢、红丸男权的荒谬，却同时在跑步机汗流浃背地幻想着六块腹肌的荣耀。他们错失了什么？

- Table of Contents
从“和解”到“生存”的自助文化
吞下红丸，拯救国家
新保守主义后女性主义：装模作样赚流量
显化之力？

[image]

“你若盛开蝴蝶自来”、“谁痛苦谁改变”、“接受你永远不会被爱的事实”、“向内求，无往不胜”、“构建强大的心理防线，你将坚不可摧”…… 你一定听过类似这样的论调，它们几乎无处不在。其唯一作用只有：自我维稳，和被强摁下去变得更加深层、更加苦不堪言的伪装。

这些诡异的说辞将你所经历的统治压迫的困苦完全归咎于你的个人“修养不足”，当你开始垂下头来进行自我检讨时，一大堆“自助励志专家”蜂拥而至，禅修茶艺、瑜伽密宗、形象管理、灵修操练 …… 争先恐后掏空你的口袋的大师们宣称他们掌握着帮你摆脱困苦的唯一出路。

这些被称为自助文化的“新风口”在算法操纵的性别极化的数字世界里迅速扩张。“自助大师”绝口不提压迫性系统构筑的人际高墙和对人心的摧残，他们只需要你相信他们所提供的是针对亲密关系危机的“最佳解决方案” —— 其基于生存主义的个人主义与性别本质主义的“务实性”话术阻断了几乎所有质疑。

[image]

这种诡异的现象并不仅仅是数字时代某种拉流量的赛道。它产生于一种新自由主义的“照护赤字”之中 —— 在这种情境下，系统性的不安全、社会的碎片化、以及 互助基础设施 的侵蚀和缺位，使个体 不得不独自应对 集体性的问题。

在这样的环境中，“红丸”意识形态与新保守主义后女性主义 相互汇合，将个人发展转化为一种在不稳定世界中求生的策略 —— 这一策略日益呼应着塑造 当下全球新法西斯政治 的现实。

[image]

本文作者是土耳其籍社会学博士后研究员。

[image]

如今，全世界的人都在被社交媒体上的自助励志大师所包围，这些家

伙向你最私密的困境兜售“速效解决方案”。其中，关于如何恢复“女性能量”或“男性力量”的建议尤其流行，声称能让你在爱情、性、金钱乃至整个人生中取得成功。这绝非某种随意的流行趋势。它直接回应了新自由主义时代导致的普遍的不安全感 —— 在这个时代，每个人都被迫自责、被驱使着自己去处理系统性的问题。越来越多地，这种文化已经开始走向一个更为阴暗的方向，呼应着关于权力与控制的威权主义观念。

“照护赤字”这一术语由女性主义学者提出，指的是维持我们的福祉所需的资源、时间和社会联系的系统性短缺。它表现为疲惫、情绪困扰，以及对市场化和个体化补救措施的依赖。“自助文化”的普遍存在，是新自由主义语境的一个副产品 —— 在这一语境中，福祉被视为个人责任，而“自我提升”则被视为道德义务。

与此同时，自助意识形态还携带着威权倾向，然而目前为止这一点在学术界和公共讨论中还未能受到足够关注。它抬高了自助“专家/网红”的权威地位，这些人往往很接近那种魅力型民粹主义政客，而这种影响力又被社交媒体平台所营造的情感亲近幻境进一步放大。并且，这种关联并不止于此。

从“和解”到“生存”的自助文化

自助产业与新自由主义之间存在两种关联。

首先，它通过创造一种利用人类脆弱性的经济，为照护赤字提供一种暂时性的修补。其次，它通过提出“自我与关系应像企业一样被管理”的观念，将新自由主义思想引入每个人的私人生活。随着公共和社区照护基础设施不断被侵蚀，线上自助资源已成为重要的应对机制，尤其是在正规心理治疗对许多人来说在经济上难以承受的情况下 —— 在全球南方尤为如此。

在20世纪90年代和21世纪初，自助文化强调沟通、情感反思以及和解，将其视为“实现”个人和职业成功的路径。这种取向与新自由主义

吸纳并商品化进步价值的那个阶段相一致。本着这种精神，流行的治疗话语鼓励男女将传统上被视为“阳刚”的特质（如果断和自主）与传统上被视为“阴柔”的能力（同理心和关怀）相结合。

然而，当代自助类作品却呈现出显著的转变，其倡导的自我认知更具本质主义和权威主义色彩。女性气质与男性气质不再被视为需要调和的特质，而是被视为应当在其性别特有的身体中得以复兴的“真实自我”。这种“复兴”逻辑基于一种诊断，即：个人及人际关系问题源于男女在现代生活的腐蚀性影响下，脱离了其所谓的“自然状态”。

这种诊断进一步呼应了当代威权政治中那些关于“性别秩序”和社会凝聚力“面临更广泛危机”的危言耸听论调。呼吁恢复所谓“阴性”与“阳性”能量的主张，不仅被视为解决个人及人际关系问题的“良方”，更支撑着与新保守主义政治相关的更广泛的道德议程，其中包括反性别运动以及针对非二元群体日益加剧的敌意。

另一个关键问题是，在自助话语中，极端个人主义和生存主义思潮正呈激增之势。丹尼尔·内林（2024）指出，这种动态是在全球新自由主义危机背景下形成的，这场危机以经济不安全、社会原子化、以及对制度信任的下降为特征。因此，一种以生存主义为导向的个人发展方式日益凸显，这种方式在充满冲突与危险的反乌托邦世界中，将自我保全与自我满足置于首位。在此背景下，个人发展“并非关乎在理性世界中蓬勃发展”，而是“关乎在失序的世界中获得你真正想要的东西”。

[image]

催婚逼婚、政府强化父权制“核心家庭”、将“不合规”的性行为刑事化处罚的男性主义复兴政治，与社会普遍的性别焦虑交织在一起。

传统性别关系的动摇和新自由主义不稳定性所引发的挫败感弥漫着整个社会。

伴随这一切的，是一种对强大父权人物/强人政治的渴望——这一人物被想象为国家与家庭的双重首领。

在这一背景下，作者考察了土耳其自助类情感关系内容网红以及他们兜售给大众的建议。在这一语境中，一种新保守主义版本的后女性主义（即中文讽刺为“田园女权”的派系）与“红丸意识形态”作为两种相互对应的性别框架浮现出来。两者都呼吁“回归传统”性别角色，同时强化个人责任与“自我提升”的新自由主义观念。此外，它们还倡导一种生存主义和战略性表现，这种观念基于对不平等与不稳定状况的务实却片面的认知。

[image]

吞下红丸，拯救国家

“红丸”一词源自经典电影《黑客帝国》，在那里，选择红丸象征着觉醒 —— 看清大众熟知的世界其实只是幻象。红丸意识形态在致力于男性权利行动、男性自我优化以及厌女世界观的网络空间中发展壮大，这些空间通常被称为“男性圈”（manosphere）。这些空间传播一种信念：女性本质上具有操控性，而女性主义应该对社会与道德的衰败负责。

红丸意识形态可追溯至2010年代初，与全球新自由主义危机的开端相吻合。它将当前局势框定为一种“男性气质危机”，这种危机据称是由女性主义、“觉醒文化”、以及据说偏袒女性的法律与社会规范所引发。

如今，红丸意识形态在全球传播，吸引那些将其视为理解自身情感挫折、经济焦虑以及更广泛不满的一种方式的男性。

[image] [image]

重要的是，红丸本身也作为一种男性“自助”形式运作。它提供一套实践脚本：锻炼肌肉、提高睾酮水平、追求经济独立、压抑情感脆弱性，以及避免对女性产生深层依附。在这一框架中，“自我提升”成为在一个被描绘为敌对且对男性不利的世界中进行防御和支配的策略。

[image]
[image]

我们不能简单地将红丸视为极端厌女。

正如西蒙·科普兰（2025）所指出的，其吸引力在于它能为“男性的抱怨”提供结构和意义，将个人挫败转化为集体不公，

并将男性的不满组织为一种共同身份和使命。

在这里，“生存”成为核心目标：逃离屈辱、重新获得控制，

并为一个男性权威能够恢复的“未来”做好准备。

“男性圈”叙事记录了当下的不公与痛苦，但却将其根源归因于社会的“女性化”。进而，这些叙事将生存主义和军事化的男性气质推到了前台。

在这一过程中，“红丸”思想将性别本质主义与厌女、种族主义、排外主义以及极右翼政治结合在一起。末日叙事与危机想象进一步强化了这种男性主义精神，将支配、等级制度以及为冲突做好准备视为应对这个破碎世界的必要反应，从而赋予其正当性。

在土耳其语境下，“男性圈”的领军人物是塔辛·奥古兹·阿卡图尔克，他在YouTube上以“红丸博士”作为昵称，该平台也是他施加影响力的主要阵地。他所倡导的“红丸”理念尤为引人注目，因为他围绕“道德复兴”这一核心思想，将个人生存与国家生存紧密联系在一起。

[image] [image]

网红阿卡图尔克的民族主义在很大程度上是象征性的且去政治化的。他避免评论国家层面的政治，以便保持一个广泛的受众群体 —— 否则这些粉丝可能会因激烈的政治极化而分裂。他经常将服兵役和采矿等高风险劳动视为“男性气概”的重要标志。然而，这种修辞抹去了这些劳动的阶级与政治维度。他一再忽视这样一个事实：在土耳其履行强制兵役的人、在监管不力的矿井中冒着生命危险辛勤劳作的人，是工人阶级的男性，而非像阿卡图尔克这样的中上层阶级男性。

然而，他的红丸建议假设了一种中产阶级主体 —— 拥有足够的时间、足够的收入和稳定性来投入持续的自我优化。这种假设忽视了过度工作（996）、经济不稳定（生活成本问题）与焦虑抑郁（甚至抑郁经济）等现实，这些现实塑造了许多本地男性的真实生活。其结果就导致了一种"残酷的乐观"：赋权的承诺注定会对那些缺乏结构性资源的年轻工人阶级男性来说无法实现。

[image]

阿卡图尔克经常强调男性作为士兵的社会角色的重要性 —— 即保卫和为国家而战，这被用来证明男性的优越性。围绕战争、自然灾害与混乱威胁的恐慌叙事与之相伴。通过强调服兵役这一民族主义的经典母题，并动用国安语言，他提出女性在根本上依赖男性的保护。

但随之而来的前提是：女性必须"值得被保护"。由此，他提出女性应服从男性权威，并在国家认同的道德框架内规范自身行为，才配得上男性的军事牺牲。

阿卡图尔克对女性的看法源于土耳其现代化进程中长期存在的道德焦虑，即"女性的行为象征着国家的道德纯洁性"。基于此，他谴责那些据称将现代性等同于夜生活、饮酒或与男性社交的"解放"女性。然而，他的主要矛头指向女权主义者 —— 在他看来，女权主义者不仅要为土耳其社会所谓的道德崩坏负责，更因"阉割"男性而激化了针对女性的暴力。

[image] [image]

新保守主义后女性主义：装模作样赚流量

后女性主义可以被理解为一种新自由主义回应，它利用女性的赋权诉求，同时宣称女性主义的主要目标"已经实现"，从而使集体女性主义政治显得不再必要且过时。它并非任何集体身份，而是一种通过媒体话语生产的文化感性。

正如罗莎琳德·吉尔（2007）所指出的，后女性主义的敏感性充满了深刻的矛盾。它一方面颂扬女性赋权，另方面却将女性气质视为一种需要不断完善以获取“成功”的个人资产。因此，赋权不再关乎集体斗争或结构性变革，而是关乎个人自我管理、自信与成就的问题。

直到最近，后女性主义文化还在利用包容性、身体积极主义以及“女强人”等进步主题。它将部分女性主义思想重新包装并嵌入到消费主义之中，并将其内容掏空，从而塑造出“坚强独立的女性”这一肤浅的陈词滥调。然而，如今后女性主义话语正发生显著转变。它们越来越多地拥抱传统的女性理想。

在这个新版本中，“传统妻子”美学与极致女性气质成为了赋权、自主选择和自我实现的标志。它们对女性的吸引力还在于承诺能摆脱有偿劳动。然而，这一动态同时重新确认了父权制关于女性可欲性与家庭角色的规范。因此，它顺应当下保守主义和男性中心主义复辟的潮流，对新自由主义的女性理想进行了更新。

这一语境的独特之处在于，它提倡的是一种策略性的、犬儒世故且务实的女性气质。理想的女性特质不再仅仅是道德美德或自我牺牲的表达，相反，面向女性的自助指南将这些特质重新界定为女性可以战略性运用的工具资源，用于生存并实现成功。

例如，效仿“红丸”信徒的约会套路，女性约会博主们鼓励女性释放自己的“黑暗女性气质”，这指的是女性据称“与生俱来的”诱惑、情感操控和掌控的能力。此处的目标不仅仅是获得浪漫关系 —— 这些博主公开将“钓”到“高净值”男、并迫使男人们为你爆金币，作为女性的一种“财务策略”。

土耳其知名励志博主埃斯拉·埃兹梅奇恰如其分地体现了“战术性女性气质”的兴起以及后女性主义向新保守主义的转向。尽管埃兹梅奇主张“性别平等”，但她认为，女性在公共生活和就业市场中的平等参与反而削弱了她们的“女性特质”。在她看来，传统性别角色的动摇削弱了人际关系的稳定性，并导致“短择”爆发 - 降低了男性对承诺的意愿。

[image]

其结果就是，女性对恋爱和婚姻的失望感与日俱增。

作为解决方案，她建议女性通过“装”、“演”、和耍心机的手段来获取男性的情感和物质的持续投入与承诺。她建议女性应夸大对伴侣的依赖，以增强男性的男子气概；她声称女人应该持续维护自身的性吸引力与外在形象 —— 她带货的美容产品正是围绕这一目标进行销售的，承诺“增强女性气质”并因此激发男性的欲望和承诺。

[image]

总体而言，埃兹梅奇鼓励女性在伴侣关系中表现得温言软语、顺从听话，并且要看起来天真无邪。然而，这并非真正的天真，而是一种精心策划的情感克制，包括战术性地“忽冷忽热”、标高价码、不要让自己轻易可得，以及用表达失落替代争吵来维持男性的兴/性趣。

埃兹梅奇的建议中处处充斥着矛盾和愤世嫉俗。她对男性特权提出质疑，且经常将当代男性的行为描述为不可靠、自恋、逃避责任；尽管如此，她却仍然鼓励女性承担起维系感情关系的重担。例如，她从道德上谴责男性的不忠，却认为这可以通过女性的“自我提升”来预防 —— 你要是“很会、很美、活儿好、有价值”，他就不会走。

埃兹梅奇呼吁读者去理解“男性本性”及其所谓的当代退化。声称女性应当通过与父权制达成新的妥协，据此来塑造自己的诱惑值和“恋爱艺术”。此处的根本矛盾在于，她建议女性付出繁复的情感和身体劳动，正是为了吸引、掌控并留住这些“有缺陷”的男性。

埃兹梅奇的后女性主义具有新保守主义色彩，因为它排除了对性别不平等和基于性别的暴力的政治意识及结构性理解。她将赋权定义为“个人成就”，这取代了集体的女性主义斗争。相反，她鼓励以一种玩世不恭的态度展现传统女性气质，以此来维持男性的关注，尤其是那些在经济和情感上慷慨大方的富有男人的关注。

然而，埃兹梅奇及类似的自助励志类网红所提供的建议依然极具吸引力。在缺乏大众化的女权主义资源和易于获取的支持网络的情况下，女性需要此类“务实”的解决方案，才能在充满不平等且动荡不安的社会环境中生存下去。在当下，随着亲密关系中的厌女情绪日益加剧，加之反性别政治思潮的蔓延，这一点尤为凸显。

[image] 这类毒鸡汤铺天盖地。

显化之力？

当代自助励志话语推进了一种更新的性别本质主义逻辑，这一逻辑在社交媒体上找到了极为适宜的土壤。它教导男女恢复其性别特定的“真实自我”，以实现爱情与人生的“成功”。这一动态与当下的反性别主义和男性主义复兴相契合。

[image]

此外，其对“生存”和战术型心机婊之重要性的强调，揭示了在新自由主义矛盾加剧的背景下自我观念的变化。

“获得你想要的东西”的命令，在一个混乱世界中使社会残酷与工具性思维常态化。

因此，生存主义自助成功学将当下的威权逻辑带入日常生活，塑造着人们对自我的理解以及与他人相处的方式。

流行心理文化中对所谓的“自恋型人格障碍”和“反社会人格”的标签式迷恋，正是这种交汇的一个症状。它既反映了对脆弱性的深层焦虑，也体现了对支配、操控与情感控制的迷恋，这在亲密关系中唤起了一种类似法西斯主义的幻想。

[image]

流行自助励志书籍中的“显化”潮流 —— 即相信我们可以通过意念将愿望化为现实 —— 为这一联系提供了另一个鲜明的例证。常借助对量子物理的曲解进行传播，声称纯粹的心理能量就能改变物质。其主要工具是“肯定语”，即用于将思维编程为“成功”模式的咒语。

[image]

“显化”在数字世界的自助励志领域极具人气。臭名昭著的“红丸”网红

安德鲁·泰特向男性呼吁道："闭上眼睛。专注于让自己感到兴奋和充满力量。想象自己轻松地实现目标。" 在其他地方，白人至上主义者的自我肯定视频则煽动着关于男性超越性的种族化幻想："我感受到超越绝对极限 …… 感受到那种活跃、积极、坚韧、内在于神话般北欧男性气概的力量。" 而在所谓的 "神圣女性气质" 领域，女性则被鼓励通过 "女神肯定语" 成为最完美女人，以确保她们"散发出强大的磁性能量"。

[image]

这类自助类骗子们兜售的简单易行的内容创作逻辑和在线互动陷阱，在一定程度上解释了为何"吸引力法则"类内容如此泛滥。在日益难以预测且充满挑战的世界中，人们对掌控感和确定性的渴求，也是此类伎俩广受欢迎的另一原因。

[image]

"显化"理论通过宣称生存仅仅是你的脑活动，并要求每个人自己去"掌握心灵与宇宙的力量"，从而助长了社会疏离感。在此背景下，那些效仿民粹主义领袖的自助大师们，提供了召唤这些力量的"秘方"，以帮人们摆脱"次等男性气质"、"受伤的女性气质"、以及在生活中沦为无力受害者的命运。

七十年前，阿多诺（1957）曾将《洛杉矶时报》的占星专栏分析为一种伪理性媒介，并追溯了其与社会偏执及威权主义的关联。据此，这种占星指导以一种融合了理性与非理性元素的方式，捕捉到了社会现实的核心张力，并承诺提供一种应对之道。

[image]

因此，占星术的吸引力 —— 以及就我们所讨论的"显化"而言 —— 源于一种保证：在充满潜在威胁、充满对抗且复杂的世界中，"个体能够"掌握某种控制权。

然而，这种掌控感却难以捉摸。如果个人无法将积极的事物具象化，反而深陷焦虑之中，那么由于"意念胜于物质"的原则，他们的担忧很可能就会成真。由此，一种脆弱的个人力量幻想，加上对消极思想和失败的自我指责，便催生了阿多诺所谓的"依赖意识形态" —— 它伪装成个人掌控力。

[image]

相比之下，对于恐惧、焦虑、原子化社会人心的疏离、和“受害者心态”的普遍感受，在当下却迫在眉睫，它们既是如今每个人切身的苦难，也是围绕着重现的性别本质主义和极右翼政治而被动员起来的情感。

于是，我们面临着这样一个问题：如何在解放性项目中集体应对、治愈并重塑这些状态？

此处的挑战在于将生存转化为共同的抗争；避免挫败感和不安感被导向怨恨或支配，而是转化为推动社会变革的集体行动。

或许，我们面前的任务是让“实现革命”比“彰显个人力量” 更具吸引力。

[image]
[image]

当“反贼”变得越来越像他们的对手…：打破僵化的激进主义令人窒息的气氛

[image] 关键词	关系结构 反叛 反抗 变革 安全培训 安全文化 心理学 战术 无政府主义 社会控制 统治 虚无主义 资本主义
[image] 关联	
[image] 创建时间	2025年7月1日
[image] **Description**	心理安全

不要以为个必须悲伤才能成为名战，尽管TA所战的东西是令憎恶的。— 歇尔·福柯

[image]

当激进派行动者拒绝采取匿名化安全措施、甚至有意以实名身份进行工作时，仅仅将其解释为“缺乏安全意识”，就过于肤浅了，更无法解决问题。倒不如问问社区：是什么样的价值观和内部文化导致人们认为曝光度比战术水平“更具价值”？不能“变现”的幕后工作不值得做的歪理是如何产生的？被捕和被驱逐这些明显是抵抗失败的结果为什么在很大程度上被称为“勇气”和“光荣”，如此绝望和孤立的氛围是如何在反抗者群体中蔓延的？

为什么激进运动和激进团体中有时也会充斥着恐惧、焦虑、猜疑 ……自以为是和竞争？

难道加入反叛阵营的人们不正是因为认清了社会上那些有毒的人际关

系模式并不愿苟同，才聚集起来与之对抗的吗？

为什么反对者却变得跟敌人的行为方式越来越像？

…

为什么如此多人追求嘴炮高于实际行动？

为什么越来越多的人热衷于更大尺度的表现自己、着眼于人设的完美化，而不是对达成战略目标的进度做出实际的贡献？

…

如果您也曾经对某些激进派圈子感觉伤心失望、被这些问题所困扰、甚至亲历其伤害，请记得，切勿简单地归咎于人群/族群，那只会导致状况更糟。

本文译自“Joyful militancy: building thriving resistance in toxic times”，AK出版社与无政府主义研究学院合作出版。这本书在我们近期的小型研讨会中使用，现推荐给所有朋友，您可以在您的团队中进行更多探讨。并欢迎分享您的思考。

鉴于本次讨论中多有涉及私人故事，因此对反馈意见我们统一不做整理。这项工作的目的是引发思考、激励对更多新的修复方案的构想和尝试，而不是分发某种通用教程。在这一复杂问题上也不该存在一致的结论。

Joyful militancy: building thriving resistance in toxic times | Bergman, Carla;Montgomery, Nick | download on Z-Library
Read online or download for free from Z-Library the Book: Joyful militancy: building thriving resistance in toxic times, Author: Bergman, Carla;Montgomery, Nick, Publisher: AK Press, ISBN: 9781849352888, Year: 2018, Language: English, Format: EPUB, Filesize: 2.81 MB
[image]https://z-library.sk/book/5671950/fd2dcb/joyful-

militancy-building-thriving-resistance-in-toxic-times.html
[image]

这里的“快乐”并非通常所说的“幸福”，这是两种不同的东西，尽管词典里认为它们是同义词。

在帝国的世界里，“幸福”是一种征服的工具 —— 幸福被视为一种责任，而不幸福则被认为是病态的。当然，幸福也可能具有颠覆性，因为它是让□变得更有活□、更有能□的过程的□部分；但是，当幸福成为□种需要被抓住或追求的东西、成为“□命的意义”时，它往往会失去其变□的潜□。快乐则不同。如果我们不快乐 —— 如果我们抑郁、焦虑、上瘾或“疯狂”—— 我们就得修复□□，或者□少控制□□的症状。而对幸福感的渴求则会让人麻醉在统治之下。

与幸福相反，强调快乐意味着摆脱习以为常的习惯、反应和情绪。

[image]

快乐通过与征服□量的□争重塑了□们。

快乐是□种解脱，□种□命本□的强化。这是□个重获新□□逐渐□解的过程。

幸福就像□剂□醉剂，会让□产□依赖，□快乐则是□种能□的增□，

它能让□体验新的事物，并最终打破这种依赖。

正如女权主义学者西尔维娅·费代里奇曾经对幸福和快乐之间的区别进行的解释：

> 「快乐是□种积极的激情。它不是□种停滞不前的存在状态。它不是对事物现状的满□。它是感受□量在你和你周围□□上不断增□的□部分。这是□种感觉，源于□个转变的过程。这是□个成□的过程。」

统治者塑造了人们的抱负、情绪和□份认同，这就是为什么 “反抗”始终意味着必须与□□的□部分进□□争 。国家掌控着人们的欲望和□活节奏，所以要想瓦解它，仅仅“发现真相”和传播真相是不够的。

如果你想要终结统治压迫，就需要找到快乐的能力。

[image]

大约一个世纪前，著名的无政府主义者艾玛·戈德曼在一次聚会上尽情跳舞，当时一个年轻男人把她拉到一边。“那人一脸严肃，仿佛要宣布某位亲爱同志的死讯”，他告诉戈德曼：“一个激进派倡导者不应该跳舞”。他说，这会让革命运动看起来很糟糕。

戈德曼很生气，基本上是直接让那个人滚蛋了。

这次遭遇被认为是戈德曼那句著名的 “如果我不能跳舞，那就不是我的革命”的出处。

这不仅仅是关于舞蹈。戈德曼坚持认为，在激进运动内部也依然存在着墨守成规和自我维稳的现象，倾向于认为激进分子应该把 “事业”放在自己的欲望之前。

一个世纪后，尽管规则可能已经改变，但某种东西仍在许多政治空间、运动和圈子里流传，从内部削弱激进运动的力量。它表现为对自身和他人的错误与共谋的警惕性觉察；将正在发生的事件归类到僵化的框架中的悲哀慰藉；感到自己比他人更激进的愉悦、和担心不够激进的恐惧；在社交媒体上焦虑地摆姿态，享受被点赞的兴奋与被忽视的低谷；面对新事物时产生的怀疑与怨恨；好奇心被认为显得天真而居高临下的态度却显得正确 …… 我们能在某些时刻察觉到这种东西的出现，就是当我们感到需要以特定方式去表现、去憎恨特定的事物、做出“正确姿态”的时候。我们曾站在其清教徒倾向的两个极端，既是纯洁者也是腐败者。最重要的是，它对差异性、好奇心、开放性和实验性怀有敌意。

这一现象无法详尽描述，因为它始终在变异与循环。不能将它归结为某些人或行为的问题。并不是说外面有一群混蛋在扼杀运动并摧毁世

界。事实上，这种对有缺陷的人或行为的警惕性搜寻 ——以及在任何地方曝光它们的冲动 —— 更可能是毒性过程的一部分，而不是解决方案的一部分。没有人能免疫于这种情况。它被广泛地感受到，但却难以谈论，所以大声喊叫是没有意义的。它更像是一种气体：持续循环，在我们背后悄然作用，引导我们走向僵化、封闭、和彼此间的敌意。这种气体让我们咳出了确定性：有人感到被挑衅，选择攻击或退缩；有人推销止咳药；但这一切都无法阻止它的扩散。至少对我们而言，没有解药，没有防毒面具，没有万能的解决方案。

我们称这种力量为僵化的激进主义。它既是一种需要被修复的存在，也是一种修复的方式。它在试图弥补的意义上修复，将新兴运动视为本质上存在缺陷的。修复意味着将一切视为破碎，将斗争和项目视为不足。它也在使之永久化的意义上修复，将流动的实践转化为僵化的存在。

当僵化占据主导地位时，创造性就会消亡。

如今， 僵化的激进主义的一种表现形式是所谓的“好政治”的概念。【注：这一概念催生了类似于中文圈熟悉的“嘴炮”风格。】

在许多圈子里，经常能听见人们说某个人或某个群体“他们的政治挺好”。那到底什么是“好政治”呢？

[image]

当政治不再是人们共同实践的活动、而仅仅是个人所拥有的东西时，会发生什么？当共同实践总是需要被宣扬\其所谓的“良好性”需要被展示时，又会发生什么？

越来越多的情况下，所谓的“好政治”似乎只是意味着采取正确的立场、说出正确的话，在Facebook、Twitter或Tumblr上传播最激进的言辞，指责做错事情的人，以及拥有经过深思熟虑的观点。

我们被鼓励 —— 而且还经常互相鼓励 —— 把我们的政治观点和分析当作徽章戴在胸前，当作与众不同的标志。当政治像时尚一样成为一种拥有的东西时，它就总是需要“被看到”才能发挥作用。行动“需

要”被公开，立场“需要”被坚持，我们的日常生活“需要”被大声地传达给彼此。人们被鼓励根据政治承诺来衡量人设。政治成为了一种需要表演的奇观。这种现象在互联网上达到了顶峰，因为分享“正确”的内容和说出“正确”的话往往是人们相互了解的重要方式，甚至可以说几乎是唯一方式。群体需要转向内部，不断评估自己与这些理想的关系，然后将它们向外投射，宣称自己的意图、价值观、计划和使命。

但由于除非跟那些缺乏好政治的人相对比，才能凸显“好”政治，僵化的激进主义倾向于不断地比较和衡量。一般情况下如果要想避免因缺乏好政治而受辱，最佳方式就是找到在激进主义、反压迫或其他理想方面表现不足的人。现实中一个人的政治德行可能永远无法完全符合这些完美主义的理想，因此他就不得不承受持续的羞耻和恐惧。

【注：华语朋友可能熟悉的“公德私德”评判，很大程度上就起源于这样的逻辑。以至于它很快就被敌人利用了。这种情况下聚焦于任何个人和行为的争辩都无从解决问题，只是分散了对问题根源的关注。】

当激进分子在所谓的“好政治”的游戏中相互攻击时，这在一定程度上是因为这里是一个人们可以行使一定权力的场所。即使一个人无法挑战压迫性结构、即使一个人无法参与创造替代性的生活方式，TA仍然可以因各种原因批评指摘/攻击周围人，并告诉自己这些攻击本身就是“激进的”。

在所谓的“好政治”与僵化激进主义的博弈中，“对手”并非资本家、种族主义者、政府警察这些压迫者，而是那些争夺批判和对抗资本主义、种族主义及警察国家的方式“是否正确”的其他群体。

[image]

对不同阵营或思潮的比较与评判可能变得如此频繁，以至于已经成为了目的本身：每次遇到新思潮时，都下意识地以怀疑的态度寻找其缺陷。我们对他人的“认识”——他们的信念、承诺和价值——只是基于他们如何擅长描画立场（俗称“站队”），并将其与我们自己的立场（“队形”）进行对比……这真的靠谱吗？

[image]

从这个意义上说，僵化的激进主义并非一种政治思潮，而是一种渗透到当今许多不同思潮和环境中的倾向。在某些环境中，所谓好政治的标准是明确地（或通过行动展示）对采取直接行动、起义、破坏财产以及与警察发生正面冲突的意愿。在其他环境中，则是进行反压迫分析的能力，避免压迫性言论、以及揭露那些发表此类言论的人。在另些圈子中，它是避免工作并靠不买东西或不付房租生存下来的能力。在某些圈子中，它指的是坚持一种“左翼的”或革命的愿景；而在其他圈子中，它是认为左翼已死、革命是荒谬幻想的信念。在某些圈子中，它是指参与过许多项目或与一个庞大的激进组织者网络有联系的能力 …… 在每种情况下，都存在一种倾向，即一个圈子会贬低其他圈子的承诺和价值观，并揭露其不足。在极端情况下，这会催生出一种宗派主义，而公开发表宗派风格的言论本身就加剧了这种宗派主义。

新人立即被置于一种负债累累的地位上：欠下奉献、自我牺牲和正确分析的“债”，必须通过不断证明自己以“偿还”。无论是对反压迫言语的表演、对革命热情的展示、虚无主义的疏离姿态，还是隐含的着装规范，那些不熟悉圈子期望的人从一开始就注定失败，除非他们“追赶上来”并顺应。无论是微妙的还是明目张胆的，新人都会因“犯错”而遭到攻击，被嘲笑、被排斥，尽管这些人往往正是“好政治”本应支持的对象：那些缺乏正式的教育培训、未曾接触过激进派社区环境，却对反抗斗争有着切身利益的人。

这一切并非暗示我们应对压迫采取更模棱两可的态度，更不是说坚定的立场有什么错误，也绝非暗示所有激进实践都是腐败或不良的。相反，我们真正认为，发展分析、指出错误、参与冲突都是不可或缺的。打破僵化的激进主义并非呼吁“和睦相处”或者“闭嘴干活”或者“随性而为”。这绝不是呼吁减少激进主义。人们挑战和摆脱压迫性行为、采取直接行动，或避免出卖劳动力和支付租金的能力，都能在主导性的统治秩序中创造并加深裂痕。这些行为都可能具有赋权的意义和变革性。但任何这些实践也可能成为比较和评估的标尺，最终贬低其他实践并抑制集体能力的成长。

由于僵化的激进主义在各个领域都引发了一种责任感和义务感，人们总有一种感觉，觉着自己永远做得不够。在这种背景下，“倦怠”在激进主义空间中不仅仅是由于辛勤工作而感到疲惫；它往往意味着受伤、耗尽和磨损：“我特么快要被烧光了。” 耗尽我们的不仅仅是长时间的工作，还有羞耻、焦虑、不信任、竞争和完美主义的倾向。正是

这些倾向扼杀了集体创造力和变革的能力。通常，说自己已经精疲力尽是退隐、休息、自我照顾并远离这些竞争动态的最安全方式。

公开讨论这些问题是有风险的；总有可能被贴上自由派、压迫者或反动派的标签。正因此，许多关于这些问题的讨论发生在彼此足够信任的个人之间，他们知道说出来不会立即遭到怀疑或攻击。在这些较为私密的对话中，有更多空间进行质疑与倾听，容纳细腻、微妙与关怀——这些在僵化的激进主义盛行时常常被忽视的元素。

[image]

本书收录了作者在与各种不同社区的激进派活动家的对话中提出的问题和交流：僵化的激进主义是如何运作的？它的轮廓是什么，它的来源是什么？是什么触发了它，又是什么让它传播开来？如何才能避免它，又如何才能激活其他修复方式？

[image]

当政治在一个被高度曝光和僵化所主导的世界里运作时，有大量事物被忽视，且永远无法被计入，即：人们在无人注视时所做出的非凡之举、人们在默默无闻中相互支持与关怀的方式、与其他生活与抗争方式相遇时所产生的犹豫与忐忑……所有那些匿名的抵抗和行为，需要数年甚至数十年才能完成的缓慢变革历程，以及所有那些无法用语言完全捕捉或公开展示的难以言表的运动、斗争与项目。

僵化的激进主义阻碍了共同学习、倾听和质疑，也阻碍了我们摆脱屈从（我们根深蒂固的习惯）。它阻碍了我们艰难地恢复和发现责任，也阻碍了我们建立基于信任和关怀的关系的能力。所谓的“好政治”的游戏只会使得培养谦逊之心、积极的响应和创造力变得更加困难。没有人能够拥有这一切。欢乐的共同理念永远无法被占有；它们只能通过集体努力来发展和维护。它们是在变革性的关系结构和斗争中不断成长的共享力量。当它们被视为高举的荣誉象征或被紧握成身份标识时，它们便会死亡，脱离了赋予它们生命力的过程和关系。

僵化的激进主义扼杀了快乐：它通过强加外部规范和标准、滋生不安全感和焦虑，耗尽了人们的活力。最大的悲剧在于，它将一种活生生的且应该始终都在不断成长的激进主义转化成了一种窒息的理想，如同一个永远在视野中、遥远的且渐行渐远的地平线。

这些倾向导致许多人放弃了激进主义圈子。僵化的激进主义带来的是可能性的不断收窄：要么继续在窒息且耗尽精力的氛围中生存，要么离开并尝试接受帝国所提供的生存方式。对许多人而言根本没得选，因为生存本身就与僵化的激进主义占主导地位的空间紧密相连。

从这个意义上说，僵化的激进主义可能是致命的。

与此同时，改变这一切的努力已经展开，许多人正在他们所处的环境中发起关于逆转这些趋势的对话；其他人则明确离开了小圈子，在反动的帝国与僵化式激进空间的边缘创造新的事物。通过与一群朋友断绝关系，一些人已在其他地方建立了更安静的替代方案和枢纽，这些地方能够催生新的运动形式、并重燃被压制的可能性。让新鲜空气进入的方式多种多样。

僵化的激进主义只是众多倾向中的一种，即使它目前占据主导地位。这正是本书出现的原因 - 以快乐的战斗精神为起点，并专注于此。

[image] 我们的合作者曾经在新年贺词中提出过这一论点的简略版
[image] [image] [image]

[image]
[image]

我们都很焦虑

[image] 关键词	互助 心理安全 自助 解放
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年7月2日
[image] **Description**	心理安全

[image]

[image]

建设中！敬请期待。

[image]
[image]

心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

[image] 关键词	反渗透 心理安全 社交工程 社交工程攻击
[image] 关联	[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
[image] 创建时间	2025年7月3日
[image] **Description**	心理安全

个人和团体都包括。

- Table of Contents

外部威胁
1、稀缺性
2、惧怕权威
3、提供“帮助”的渴望
4、习以为常
5、自我
6、对胜利的兴奋和对失败的恐惧
7、知识不足
外部威胁
1、肩膀冲浪
2、垃圾箱潜水
3、角色扮演
4、特洛伊木马
5、钓鱼
6、网站、在线论坛和社交媒体上的开源信息
7、逆向社交工程
逆向社交工程涉及三个部分：
最后

[image]

社交工程学有非常多的用法，其结果完全取决于目标。其中就包括当权者和间谍机构对公民施加的操纵和控制。

“如果您已成为目标”，您就必须随时留意这些迹象，以准确判断当权者的真实目的。否则，您可能会越陷越深，很快失去反击的能力。

而另一方面，在出现下面部分迹象时，您可能更加难以动员人们反抗。

那么这些威胁迹象都包括什么？它分为外部和内部两部分。

外部威胁

1、稀缺性

稀缺性指的是，人们被告知，他们最想要的东西非常有限和稀罕，要想获得它，就必须遵循某种态度和行为。他们往往不会明确指出所谓的“正当态度和行为”究竟是什么，而是向表现出让当权者满意的行为的人展示奖赏。

有些时候心理捷径是有益的，可以使人们能够更有效地应对生活的复杂性。但是，稀缺性的恐吓却具有严重的误导性。

而且，这个作用是双向促进的。当有人得到了别人没有得到的东西——比如特殊权限、食物、水，等等，就会使他们感到自己“特殊”，“独特”，“崇高”，并将这些人置于捍卫暴政的位置上。他们害怕失去这份特权。

害怕失去是一种依恋。依恋导致懦弱和奴性。

一个例子是南非政府，他们夺走了人们生命所必需的东西，并使它“稀缺” 且仅供支持政府的人可用 —— 这是一种恶意的但非常有效的操纵策略。

更糟糕的是，稀缺性创造了使稀缺性永存的心态。

穷人保持贫穷，孤独者保持孤独，忙碌者保持忙碌 …… 稀缺性创造了一种使稀缺性永存的心态。

如果所有这些看起来都很惨淡，那么另一种观点就出现了：穷人之所以贫穷，是因为他们缺乏技能；孤独者之所以孤独，因为它们令人讨厌；忙碌的人之所以忙碌是因为他们缺乏组织生活的能力 ……

用这种替代的观点，稀缺变成了深层的个人问题的结果，很难改变。而相反，稀缺性心态是因果关系的结果，更容易接受补救措施。

稀缺性本身就是环境条件的结果，而不是个人特质，这种条件通常可以加以管理从而改变它。但为什么人们却忘记了如何去改变？

稀缺性削弱人的勇气，使决策过程变得复杂，因为通常只有短暂的机会窗口可以选择稀缺的东西。所以你的全部注意力都会被吸收在那个窗口上。

这对所有人来说都是如此，不论智商如何，当看到眼前的供应开始减少时，人们就必定会感到特别有必要采取行动。经历过疫情抢购的人们应该很容易理解这点。

每种情况和稀缺性都是不同的，经常并不是厕纸和大米这么明显，当权者甚至可以人为制造出稀缺 —— 塑造公众的价值观。比如中国的户籍制度，强行将某些城市定义为高档并限制迁居。

[image]

不论如何，请随时记得，当您感知到稀缺的紧迫感时，请尝试去寻找

其成因，并想办法抵抗不平等和掠夺。而非跟随欲望。越多人认同稀缺的“合理性”，它就越容易加速深化，将所有人都拉入深渊。

[image]

2、惧怕权威

许多人在一个被视为权威的人物面前会感到焦虑，不是他们对那个人感到焦虑，而是对恐吓他们的人所代表的地位和权力。

于是攻击者很擅长假扮着执法人员或公司高级官员之类的权威人物，以从受害者那里提取敏感信息。这是一种长盛不衰的社交工程手段。还记得那个电影吗？《Der Hauptmann》那不是虚构的。

恐惧和服从并不是攻击者 “植入” 的，而是来自人们根深蒂固的对权威的下意识反应。攻击者所做的只是启发了你内心的冲动。

[image]

返回：👄套话：5种有效的社交工程启发术

返回：[image]如何欺骗，和如何防骗：反侦基础课 S06E07

学习这些知识可以帮助您理解操纵者的手段，并随时控制自己的行为。

3、提供“帮助”的渴望

“帮助” 这个词可能会存在歧义，因为这里所指的帮助并无关善良和爱心，准确说是在追求一种自我炫耀的满足感，“你看我知道这件事/我能做到***”。

攻击者的做法就是刺激目标人的这种满足感的欲望。

[image]

越是不怎么懂的人越希望彰显出自己懂一些东西，越是权力低微的人越渴望表现出自己的权力。攻击者很了解这点，这就是为什么他们以看门人、清洁人员为目标，以获得进入重要设施的权限，或者套出敏感的致命信息。

这在互联网上也一样。

当您显得自己“无所不知” 时，任何人都不会告诉您他们知道什么。相反，如果您让自己看起来像个白痴……几乎所有人都会努力“纠正”您的错误、试图“教导”您什么才是真。

攻击者要做的就是给目标人一种 “你比我智高一等” 的优越感，在这种感觉的熏陶下，目标人就会非常愿意吐露更多重要的敏感信息。

这种手段屡试不爽。尤其是通过社交媒体这种激发表现欲的媒介 —— 您只需要稍微装傻，就可以轻松获得很多人隐秘的知识和重要信息。

总之：请随时留意您说出的每一句话，使用对抗性思考方式 —— 即：考虑如果恶意者听到/看到了你所说的，他们可以用此信息来做什么。

4、习以为常

我们所有人都遇到过某些机械性的工作，即执行一组指定的活动，仅此。这会使每天重复执行相同任务的人感到无聊，并且随着时间的流逝，这种无聊感会促使您在满足目标的同时以最小的努力来完成任务。

这就导致了一种很随意的态度，并且容易受到攻击。这些攻击者将此类人作为目标，知道他们可以轻松获得攻击者所需的信息。

习以为常感会冲淡人的态势感知力，甚至其中一些人开始向 “身边人” 倾诉自己的无聊，以获得心理层面的呼应。但是他们忘了，对他们自己来说 “习以为常” 的东西，对外人来说经常是稀奇和新鲜的。听者会传播这些信息，从而被攻击者捕获。

[image]

如果您是组织中的负责人，请尽可能安排您的队友在不同时间段内做不同的工作，并同时制定严格合理的安全标准，以避免恶意者借助无聊情绪来渗透你的组织。

如果您是工作者，请随时提醒自己保持警觉，主动转移一下自己的侧重，做一些其他的事；让好奇心保持在足够的高度上。好奇心是敏锐的驱动力。

5、自我

如果您怀疑地球不是圆的而是平的，我就会努力 “为你证实” 为什么地球就是平的。这样一来您就会特别喜欢我，因此不会意识到我这在对您做什么。

这也是一种特别常见的攻击方法。包括在信息战心理操纵中都会使用这点。

举个例子。我制作一个博客/公众号/频道，我对目标受众群体做出了充分的调查 —— 我知道他们信任什么和不信什么、他们的主要观点和认知，然后我就会借助这个平台不断强调和重复目标受众群体的基本认识；这种情况下我会迅速拉拢所有人，甚至更多人。因为我的陈述 “证实” 了他们的想法。

不论这个想法有多么荒谬。

这就是社交媒体营销常用招数 —— 不断重复每个人都知道的常识，排斥一切新的完全不同的信息的输入。增粉大法。

在本集的主题上，增粉并不是目标，操纵才是。在心理战术中，当我能成功博取目标受众的信任时，我将开始渗透我想要你相信的主张。这种情况下人们已经对我操作的博客/公众号/频道具有足够信任，来自这里的任何信息都更加容易被赋予同等的信任。当然，这需要微妙地逐步地进行，而不是一次性灌输，让人们跌眼镜是不会成功的。

再一次，这种手段在那种旨在促进表现欲的媒介上使用会特别高效，比如社交媒体。在这里，大多数人仅仅是希望证实自己的判断，从而获得更强大的自信，而不是学习新的不同的东西。

我们一直被告知，保持自信，以避免恶意的误导。在很多时候它是好事，但也有一些情况下，比如上述这类操作。自信会导致更容易受到攻击。

攻击者会想办法促进目标人的自信、让目标人对自己的感觉的真实性更加有把握 —— 从而消除了对正在发生的安全漏洞的逻辑意识。

结果是，被黑客入侵的人在提供攻击者所要求的内容时不会感到任何伤害。

[image]

此类攻击之所以能成功的原因就是，攻击者拉低自己的位置，扮演受害人的听众，他们帮助受害人构建偏执的自信。

自我不会消失，但它是否会使您变得脆弱，取决于您如何处理它的具体情况。

6、对胜利的兴奋和对失败的恐惧

这两者是一回事。

如果您被告知很容易可以赚到钱，但只在一段很短的时间内有效，这

就容易被激发冲动去做出傻事。

出于兴奋，安全意识被关闭了，链接被点击，下载了恶意软件，该恶意软件使攻击者可以远程访问您的设备，您的钱、数据、等等一切都被拿走了。

快钱的确存在，但可惜不是给您的。而是攻击者的。

这种手段听起来太容易避免了，“我不贪心不就行了吗？” 不一定。它会与上述各种手段结合起来使用 —— 比如，在疫情最危险的时刻，攻击者声称现在您可以从这里买到合规的平价口罩，也就是利用稀缺性，想想看，有多少人会上当？

大型灾难期间是攻击最频发的阶段，因为这样的阶段存在广泛的天然的恐慌情绪，这份情绪是让人们失去理智的重要因素，导致很容易受到攻击。

[image]

解决方案其实很简单，对多数社交工程攻击都有效的抵制措施，即：在做出任何重要决策之前，停3分钟，思考一下，或者仅仅是转移一下自己的注意力到别的地方，稍后再回来重新考虑这一决策。蜥蜴脑能掌控的仅仅是这几分钟。时间就可以摆脱它的控制。

7、知识不足

花点时间思考就能避免攻击吗？是的，很多情况下的确如此；但是，也有些情况下，并非这么简单。

如果您对当前状况的知识不足，不论花多少时间思考，都有可能做出错误的决定。

这就是为什么恶意者总是倾向于降低目标人的知识含量 —— 您知道的越少，就越容易接受操纵。包括独裁者，都会致力于保持民众的无

知。

无知分为两种，一种是被动的无知，就如上述这样，被故意的信息封锁和瞒骗所侵害；还有一种是主动的无知，即不愿意接受那些与自己的固有想法相悖的新知识。后一种比前一种更可怕，也更常见。

最简单的例子，每个人都可以查找一下自己曾经买过的书，它们中大多数肯定具有某种共性，很可能围绕着同一种意识形态/思考方式/专业/等等。这是因为人们会下意识地寻求书籍和类似“正规信源”来证实和强调自己的固有想法。

多学习些不同的东西并没有坏处，尤其是对于有事业理想追求的人来说，实现您的理想所需要的知识肯定不止一两种。

以轻松的方式收集（并传播）知识。尽力而为。

[image]

外部威胁

1、肩膀冲浪

肩膀冲浪是一种很常见的攻击形式，尤其是在每个人都专注于自己的手机的时代 —— 攻击者使用观察技术来获取信息，同时他们正在执行涉及令敏感信息可见的某些操作。

而且可以使用双筒望远镜或其他视觉增强设备在近距离和远距离执行此操作。

尤其是需要注意，不要在公共场合从事任何重要工作，包括不要登陆自己的真实网络账户。

[image]

当您在咖啡馆里准备选一个座位时，请首先注意自己的背后和四周，是否有其他位置可以看到您的电子设备屏幕；

当您在公交车/地铁上时尤其需要注意，不要打开手机，更不要执行任何输入密码的操作，哪怕只是登陆社交媒体。

排队购物时更是如此，因为您不可能指责站在您后面的人。

[image]

返回：[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

2、垃圾箱潜水

这应该无需赘述了。如今大多数人都明白，在丢掉垃圾之前应该检查一下，那里面是否存在对潜在恶意者有利的东西。我们发现中国网店上出售遮盖物流包裹上的标签的工具（那个东西没必要买，一只打火机就可以做到同样的事），至少显示市场已经对隐私安全有所关注。这是好事。

但对于垃圾箱潜水的威胁性来说，并没有那么简单。关键在于，您的对手认为哪些东西才是致命的，而不是您。这不总是很容易判断的。

再次引用上述“内部威胁”中的“习以为常”原理，当事人对于自己熟知的东西往往会放松警惕，尤其是与其个人利益相关性不大而是与其所在组织利益密切相关的东西。比如建筑物施工图、考勤表、其他人的购物回执等等。

对于攻击者来说这些东西中都包含大量的可用信息。

这就是为什么 垃圾箱潜水经常能为情报收集带来最丰厚的回报 ，而且经久不衰。

人们经常会随手扔掉发票、通知、信件、CD、废弃的计算机、USB密钥以及其他东西，这些东西可以为真正的攻击者提供惊人的信息量 —— 不论是关于目标人的、还是目标项目的参与者、还是整个组织网络。

普通的碎纸机并没有用，更不用说简单地撕碎了。渴求情报的攻击者都具有非凡的耐心，也有足够的时间将碎纸重新拼接起来。

请随时注意丢弃的东西，在哪里以及如何丢弃的问题。使用可以切成细碎的碎纸机会很好，当然，简单地焚烧都是可以的。丢弃电子设备之前请砸烂它们，越烂越好。

[image]

返回 - 镇压手段：[image]隐蔽性地突袭住所

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法S03E06

3、角色扮演

角色扮演是社会工程师的关键武器之一。它涉及通过使用在线聊天会话、电子邮件、电话、或您用于与其他人进行交互的任何其他途径，来说服、诱导、欺骗，以收集信息。

其中社交工程师有可能扮演咨询者或技术人员的角色、也可能是无助的可怜人、或其他任何可能的方式，具体取决于对目标人弱点的分析。在这种情况下诱使目标泄露机密信息。

保持警惕的同时您也完全可以提供虚假的信息给对方。

随时记住意图是什么。意图是情报和反情报行动的关键要素。

4、特洛伊木马

这是犯罪分子和政府间谍使用的最主要方法之一，其中涉及诱骗受害者将恶意文件下载到他们的电子设备上，攻击不一定会立刻进行 ——而是在其上创建后门，攻击者可以在日后随时使用它，从而可以完全访问受害者的设备。

在零日漏洞作为最强地缘政治军备竞赛的时代，保持数字卫生应该是每个数字产品用户的基本素养。

[image]

返回 - 镇压手段：恶意软件

返回 - 自卫措施：[image]数字技术限制和最佳实践

以及，如果您怀疑设备被入侵：[image]计算机和移动设备取证

5、钓鱼

网络钓鱼一般是指创建和使用虚假的网站和电子邮件地址的行为，这些网站和电子邮件的外观看起来非常像是来自知名的合法企业、金融机构和政府机构，以欺骗接收者泄露其真实个人信息。

将您的电子邮件客户端设置为接收纯文本电子邮件，而不是HTML格式。

仔细检查电子邮件中的任何网址。虚假地址可能只是一个字母不同或缺失。

[image]

返回：[image]如何欺骗，和如何防骗：反侦基础课 S06E07

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法 S03E06

[image]

返回 - 工具：[image]URL 检查 ；[image]自动检测链接是否安全 ；

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法 S03E06

6、网站、在线论坛和社交媒体上的开源信息

有关组织结构（正式和非正式）、电子邮件地址、电话号码的大量信息都可以在网站、论坛和社交媒体上公开获得。攻击者可以使用此信息来完善其方法，并瞄准最有可能成功的目标人、制定最有可能成功的策划。

开源情报的诸多演示已经足够证明这点：关于社交媒体有多可怕。根本性的也是最简单的解决方案就是，不要使用任何社交媒体和在线论坛。

但对于大多数组织和个人来说，这不现实。于是最好的做法是分身，尤其是在不同的社交媒体上采取不同的身份，避免将个人信息集中在一处。

[image]

返回 - 自卫措施：分身

7、逆向社交工程

逆向社交工程学攻击是指这样一种攻击，其中攻击者说服目标他或她有问题、或将来可能遇到特定问题，并且攻击者已准备好帮助解决该问题。

逆向社交工程涉及三个部分：

- 破坏活动：攻击者获得对系统的简单访问权后，破坏了系统或使系统看上去受到破坏。当目标人看到系统处于损坏状态时，就会开始寻求帮助以解决问题。

- 营销：为确保目标准确寻求攻击者的帮助，攻击者会给自己打广告自称为唯一可解决问题的人。

- 支持：在此步骤中，攻击者获得了目标的信任并获得了对敏感信息的访问权限。

当您的系统出现故障时，恰逢某人在适当的时间出现以帮助您解决问题，那也许是好运，但也请考虑其故障的真正成因，也许它是某种“虚假困境”。

最后

基本上就是这样。这些威胁有可能并非单独出现，而是结合在一起、尤其是结合在一套逻辑完好的攻击策划中。

但它们的出现都具有一定程度的迹象。您需要做的就是保持批判性思考和警觉的意识。尤其是当攻击针对群体操作时，周围人的想法和行为很可能对您产生影响。希望每一位阅读过本文的朋友都能成为组织中金丝雀。

[image]
[image]

如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”

[image] 关键词	社交工程 防御
[image] 关联	👄语言是强大的武器 - 如何使用它？人性黑客：致命的诱导；[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病；[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛 ；[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年7月4日
[image] **Description**	心理安全

如果真的不想被骗，那就有必要知道该怎么骗人。继续社交工程攻击实践。本文的效果应该是鸡皮疙瘩，如果您读完后没有这种反应，只能怀疑是没能深入理解它……

- Table of Contents
诱导的含义
诱导的效果如此之好的原因如下：
开始——
诱导很简单
关于掌握交谈的艺术，最需要的 3 个主要步骤：

[image]

有效地引导别人把话说出来，是社交工程操作成功的关键。当人们和你交流的时候应该感觉很自在，制造这样的交流环境，人们就更愿意说出真话了。

审讯执行者在接受培训的时候也会被这样告知。

你也许在电视电影中看到过很多严肃的审讯场面，事实上真正的审讯往往不是那样，一开始审讯者会有意制造气氛让被审者放松情绪，这样才更容易套出真话。

这就是社交工程的伎俩。

你是否碰到过这样的人，简短的交谈后你忽然感觉，“哇，我喜欢这个人”。为什么会这样，你有没有想过？他究竟有什么特质让你产生了这种感觉？是他的微笑、他的长相、他对待你的方式、还是他的肢体语言？或许是他与你的想法及期望值比较接近？他看你的眼神比较平和，没有偏见，你此刻觉得和他在一起很放松。

现在设想你也有这样的潜能，并能掌握这种能力。 请不要以为本文在讲述如何与周边人搞好关系，不，那不是我们的主题。我们想要说的是诱导—— 让你在下意识的情况下吐露关键（也许是致命）的信息的方法。

诱导是间谍、欺骗大师、和社交工程人员最常用的技术，当然，医生、治疗师和司法人员也在使用。

如果你希望得到保护，免于圈套，或者希望自己成为一名优秀的套话大师—— 在正义的行动中作为关键能力之一，那么你就有必要掌握这些技巧。

有效地使用诱导会产生惊人的效果。

那么，什么是诱导?

它是社交工程操作中少有的针对个人的强有力的工具 ，也是将它置于社交工程框架顶层的原因之一。仅仅通过这种技巧就能改变人们对你的看法。从社交工程的角度来看，它能改变你在实践中的操作方式。

我们来试试。

诱导的含义

[image]

诱导的意思是引出、套出或者得出一个逻辑上的结论(例如某种事实)。或者，可以将诱导定义为一种引发或者诱发某种特定类型行为的刺激，就如它在“诱供”中的意思。

请再看一遍上述的定义，如果你还没有起鸡皮疙瘩的话，那么只说明理解有误。

想想它的含义。有效地使用诱导意味着你能提出具有诱导性的问题，刺激别人采取你所希望的行动。对于社交工程人员来说，这意味着有效地使用诱导可以将你说话及提问的技能提升到一个全新的层次。从信息收集的角度来讲，专家级的诱导就是指：目标愿意回答你的任何问题—— 是心甘情愿的。

我们再深入一些，所有间谍都会使用诱导的技巧，所以很多政府部门会对其公职人员进行相应的培训并给出警示，即对抗诱导、又能利用诱导达到他们自己的目的。

在国安局的培训教材中，对诱导的定义是这样的：在貌似正常和平凡的对话中精妙地获取信息。

这样的会话可能发生在任何地方，如餐馆、健身房、托儿所、菜市

场……诱导使用起来效果很好，因为其风险较低且通常很难被察觉。部分情况下， 目标甚至不知道自己在什么情况下就泄漏了信息。如果被怀疑动机不纯，则可以以“不过随便问个问题”为由假装生气、蒙混过关。目标人根本无法抓住把柄。

诱导的效果如此之好的原因如下：

- 大部分人希望自己看上去比较有礼貌，尤其是对陌生人；
- 专业人士希望自己看起来见多识广 、很有才气；
- 如果得到赞赏， 大部分人通常会越说越起劲，并泄漏更多的秘密；
- 大部分人不会为了撒谎而撒谎；
- 大部分人对貌似关心自己的人会表现得比较友善。

正因为大部分人都有这些特点，这便使得诱导的成功率极高，也使得人们在说起自己的成就时很容易口无遮拦。

下面演示一个实际操作的例子，请仔细看，社交工程师是如何使用套话技术的。

- 任务：收集某公司（组织/团队）的内部资料；该公司具有很高级别的安保系统。
- 环境：在当地的一场会议活动中碰到目标人。现场人较多，社交工程师（SE）需要寻找机会靠近目标（T）。这类会议的目的就是为了让人们互相认识，以扩展所谓的人脉，交换名片什么的，就像你知道的那种装逼聚会那样。

开始——

SE：“清静片刻？”

T：“是啊，还好有这个地方，可以坐下来喝点东西。”

SE 点了和 T 一样的饮料 —— 这个细节一般人都会，使用的是虚假帮派伎俩 https://www.pao-pao.net/article/729。

SE 伸出手，说：“我叫**（一个假名字）。”

T：“我叫**（真名字）。”

SE 拿出准备好的定制名片，说：“我是某家小型进口公司采购部的经理。”

做为回应，T 也拿出名，说：“我是 ***公司的首席财务官。”

SE 表现得很轻松，笑着说：“你是管钱的啊，怪不得每个人都在那边围着你。你们公司具体是做什么的啊？”

T 开始说起公司一些产品的情况，当说到某个知名产品时，SE 马上说：“哦，原来是你们做的啊，我喜欢那个产品。我在《 **杂志》上看到过，好像创造过销售记录啊。”（注意：这就是发起攻击前准备工作的重要性。SE 已经从之前收集的信息中了解到了这些内容，信息显示目标人自己也很喜欢那个产品，所以 SE 的赞美会起作用）

这时 T 开始显得有点骄傲了 :“你知道那个设备在第一个月的销量就超过它前后 5 个产品的销量总和吗？”

SE：“是啊，我知道为什么，因为我买了5个。”

过了一段时间，随意寒暄，保持礼貌和热情。随意的交流就能了解到很多细节，比如目标人的公司最近购买了财务软件、最近在度假的首席安全官的名字、以及目标人正准备和家人去哪里休假。这些看似没什么用的细节信息实际上有很高的价值，对下一步的攻击计划很有帮助。

但是 SE 没有满足， 继续提出了一个更为深入的问题："我知道这个问题看起来很傻，但是我们是个小公司， 老板让我研究并购买一套门禁系统。我们现在用钥匙的，但是他认为 RFID 或者类似的系统会更好。你知道你们公司用什么吗？"

注意：这个问题很敏感，很容易引起警觉。但在此处，由于上述的铺垫，加上周围气氛，以及目标人并非职业安全官，于是敏感性有一定下降。这是在计划之内的。

T 说："这个我可没有概念，我只负责签支票购买，不过我进门时用的就是这个卡 ……"他拿出钱包中的卡给 SE 看。并说，"我想可能是 RFID， 我只知道进门时晃一下钱包，门就开了。"

两个人都笑起来。

这些信息对攻击来说太有帮助了。

你可能注意到了，诱导与信息收集很相似，且紧密关联。通过良好的伪装和诱导技巧，这个特别的信息收集过程会容易得多。

[image]

诱导技巧应该使得问题能够尽可能自然地提出，目标在回答这些问题时也觉得很自然。

鉴于上述已经收集到的信息，攻击者知道目标人正在度假中、他们公司使用的财务软件类型、以及门禁系统，就可以策划出一次修复"故障" RFID 打卡机及出勤记录钟的攻击行动。

比如这样："某某（目标人的名字）在去某地度假之前打电话给我，说生产部门有一个出勤记录钟没有正确注册，我来测试并分析一下，只要几分钟就可以完成。" 对于这种大公司来说，前台不会对这种话产生怀疑。注意，要装扮成符合你扮演的角色的特征，后面还会提到这点，它很重要。

你已经看到了关于事先准备工作—— 也就是信息收集的重要性。社交媒体时代这个问题变得尤其严重了，因为太多人根本不知道应该公开说什么和不该说什么，他们把几乎一切都放在网上。我们曾经在反侦查技巧中重点强调过：任何时候不要谈论自己！但这么说似乎并不精确，因为人们可能不知道哪些内容属于"谈论自己"—— 即 可被攻击者利用的东西。举个例子。

中文网络上很多"积极人士"崇尚于所谓的"反洗脑策略"，也就是寄希望于劝服屠夫放下屠刀。我们就不讨论这个模式是不是有效了（它都傻透了），但它明显是一个很具利用价值的信息点。我们假设当局的攻击者对此比较重视。攻击者可以通过关键字搜索和汇总技术，掌握哪些人、以及以多高的频率在讨论"反洗脑"，他们的态度都是什么。选择其中相对积极的支持者作为目标对象，进一步全网探索目标人的各种其他身份细节和个人信息。把这些信息汇总起来，不论是在现实中还是在网上，使用社交工程技术对其发起针对性攻击。攻击者可以扮演"反洗脑"的支持者、甚至可以扮演挑战者激起目标人的"讨论"兴趣，进一步引诱其说出更多信息。

因为被利用的价值并不在所谓的"反洗脑"本身，而是这一想法说出的人群，绝对是异议人群对吧，于是它将关乎很多异议人士（不论其反抗能力如何）的私人信息。你还觉得"任何时候不要谈论自己"这句话很简单吗？

再一次：不要轻敌。那些被派来操纵你的人都经过非常高端的心理学培训，他们知道如何装傻以博取你的信任。尤其是在超个人主义自恋狂的时代里，你只要稍微装傻，就能获取很多人"心满意足"的侃侃而谈。这是细思极恐的。

[image]

诱导很简单

通过简单、轻松、愉快的谈话就可以从很多人口中获取颇具价值的信息。

诱导不仅用于信息收集过程，也可以强化你的伪装，从而获取信息。所有这些成果依赖于定义清晰、经过深思熟虑的诱导模型。你需要事先准备充分。模型是针对性选择的，就如我们上面给出的两个例子，通过公开信息的收集对目标人的了解，将帮助你构建最适合对方上钩的模型。这也是为什么我们多此强调：不要让陌生人太了解你！

再回忆一下定义，诱导就是攻击者想要目标做某件事，这件事很可能是简单到只是回答一个问题，也可能复杂到进入一个敏感区域。要达到这一目的，攻击者需要询问一系列的问题，其中部分是完全无关紧要的，只为了扰乱视线而存在，最终将目标人引入真正的目的。

一般秘密警察、便衣和情报机构特工都深谙此道，审讯、问询也利用这种方法。如果你经历过这些人而且不止一次，你也许能回忆到，他们使用了一些套路，就包括在上述解析中。之所以你能发现那是套路，因为他们中有些人在操作上过于机械，高手可以看出破绽。但并不意味着这些人中没有高手，也不过是你曾经没赶上高手出动。

通过上述介绍你会发现，信息是其中的关键。获取的信息越多，攻击的成功率就越高。因为诱导不具有威胁性，看起来轻松自然，所以很容易成功。请想想你在商店、咖啡馆或者其他地 进遇到过多少次那种看起来没有什么意义的简短对话？谈话的真谛在于使用诱导战术，并且每次都以一种轻松自然的的方式进行 。这也是诱导有效的原因。

此处需要提醒两个对于中国异议人士来说非常重要的事，那就是：1、你的朋友；2、你的家人。简单说就是，你自己明白如何避免被秘密警察的诱导欺骗是不完全的，攻击者很可能会从你的亲密朋友和家人角度入手，尤其是家里的长辈，他们往往毫无戒心，容易以良好的愿望出卖你。所以，你应该保持让家人知道得越少越好。还有朋友，你必须有朋友，但也需要交往那些注重安全并且和你一样理解社交工程攻击特点的人，这样你们才能形成有效的防线。

也许我们把这些骗术撕开撕碎，摆在这里，你觉得它很简单，事实上并不是。因为人的意识充满了 bugs，利用它们一点都不难。英国有一个当红的真人秀节目《骗术真相》，主要就是演示社交工程攻击是多么的容易 。攻击者扮演陌生人与目标交流，通过偷拍验证，甚至一些套路都能屡试不爽。

一切都源于交谈的艺术。这种艺术可以做很多用途，最常见的比如推销、恋爱、和老板套关系、发展人脉、医师、心理咨询、社工等等。当然也会用于诸多恶意目的。

关于掌握交谈的艺术，最需要的 3 个主要步骤：

- 1、表现得自然。

如果在交谈中显得不舒服或者不自然，会很快导致谈话失败。要想验证这点可以进行如下练习。

与他人谈论一些你精通的领域，在这个过程中你可以录像或者让朋友观察，观察你的站姿、动作以及阐述知识的方式。这些细节可以反映出你的自信和自然。

然后，尝试参与一些你一无所知的领域的谈话，同样进行录像或者让朋友观察，看看在这种对话中你试图发表“真知灼见”时，上述细节有哪些变化。

这些练习会显示出你表现自然与表现不自然的差异。对于没有专业训练的人来说，它将非常明显。

不自然的表现会葬送你成功诱导的机会。那么，如何在谈话中表现得自然？就是第二条。

- 2、你需要拥有足够的知识。

你必须了解与目标人交谈时所涉及领域的知识。此处有一个大大的!因为它非常关键。

比如，你想要得到某个绝密产品的化学成分，你要诱导的目标是制造该产品的一位化学家，并且决定和他谈论化学，那么此时你就不能伪装成一个世界级的化学家(除非你真的是)。他可能在交谈中提出一些你完全不知道该怎么回答的问题，那样你就演砸了。

最好的方法是伪装成该专业的学生，对目标人在该领域的造诣非常崇拜的那种。

重点是，不管你选择谈论哪个话题，也不管你选择和谁交谈，都要做些研究、反复练习且精心准备。一定要具备足够的知识，就目标对象会感兴趣的话题侃侃而谈。

记住，你只有一次机会！如果演砸了，那就回家吧。

- 3、切忌贪婪。

当然，诱导的目的是获取信息、得到答案或者取得进入某个领域的钥匙。然而，不要以此作为重点！

如果你一心想得到需要的信息，很快就会被目标看穿，导致目标失去兴趣。

通常情况下，给对方一些感兴趣的东西会引起对方的“交换情结”，这样对方会下意识的觉得有义务给你一些回报。在交谈中这点很重要。

交谈中要有来有往，除非对方是一个滔滔不绝的人。如果他谈论不止，就让他说。

如果你得到了一些信息，就适可而止，不要贪婪地不断深挖，否则会引起对方的警觉。反过来看就是，如果对方在某个时间点上终止了继

续交谈，你需要思考此前自己说了什么。

[image]

请记住，很多时候，世界上的“最佳的交流者”其实是那些听得比说的多的人。

还需要注意的是：面部表情，也是非常重要的。表现得太紧张或太放松都会影响人们对你问题的反馈。如果你言辞镇定，并且吸引了目标参与交谈，但是肢体语言或面部表情却表现得漠不关心，就肯定会影响对方的情绪，即使他并没有意识到这点。

你知道 Cesar Millan 吗，著名的训狗师，被称为“狗语者”。他可以与那些难以驯服的狗沟通。仅仅只需要几分钟时间，他就能让狗和人形成一些亲密的关系。他曾经提到过一个关键问题，那就是“精神”，或活力。换句话说就是，如果一个人在接近狗的时候处于精神紧张且焦虑的状态，那么即使他的言辞显得很镇定，狗也会紧张、狂吠甚至具有攻击性。这就是道理。

当然，狗和人绝对不同，但在此的逻辑是一样的。当你接近一个个体时会把自己的内心气氛带给对方，再麻木的人也有第六感，也许他们不一定能说清楚其中的道理，但他们完全可以感知到，从而下意识的在行为言谈上抱以警惕，很容易导致交流失败。

你肯定听到过这样的话，“那个家伙似乎很猥琐”，或者“这姑娘看上去很友善”，没错，这就是精神会话所传递的“感知 ”，这些信号会和个人以往的经历相关联，从而形成直觉判断。优秀的演员是深悟此道的，他们可以让自己看起来真的就是他们所扮演的角色，给你一种“他/她就是这种人”的印象。事实上完全不是如此。

如果一个便衣接受过此类培训，并完美的掌握了其中的诀窍，你可以想象得到这种事有多危险。

不是说让你对所有陌生人的搭讪都保持警惕，事实上这样做有可能无济于事。就如某些高端的网络攻击，攻击者入侵你的设备后不会立即行动让你觉察到，而是给予充分的时间，直到你忘记了自己在什么地

方连接了不安全的网络。社交工程攻击也一样，攻击者甚至可以真的和你以自然的速度熟悉起来，再发起攻击（就如我们曾经演示过的Facebook 钓鱼攻击那样），如果你只小心“陌生人”是解决不了这个问题的。攻击者甚至可以在第三方的位置，操纵你最信任的人对你间接发起攻击。

然而，攻击发起时的模式大同小异，现在你知道了其中关键的套话伎俩，就会明白该如何防备。不论这种伎俩的实施来自哪里，哪怕是亲密的人，有些不该说的东西也不能说。如果你是一个组织或团队的领导人，你应该明白如何告知掌握着重要信息访问权限的合作者和员工，防备这种诱导攻击。

[image]

语言是强大的武器 - 如何使用它？人性黑客：致命的诱导

[image] 关键词	社交工程
[image] 关联	[image]如何让一个人心甘情愿吐露重要信息？—— 社交工程攻击“诱导的艺术”
[image] 创建时间	2025年7月5日
[image] Description	心理安全

你喜欢给别人纠错吗？听到别人说出明显错误的话就有立即用事实反驳的冲动？你听到称赞自己的言语会扛不住吗？长期被忽视的你会觉得“终于遇到了伯乐”？你知道记忆能被修改吗？通过简短的对话就能实现 … 人性的弱点有可能是致命的。

- Table of Contents

  成为成功的诱导者需要几个关键要素：
  1.唤醒他人的自我
  2.表达共同的兴趣
  3.故意说错
  4、主动提供信息
  5、假装高深
  6、酒精的作用
  提问的学问
  1、开放式问题
  2、封闭式提问
  3、引导式提问
  4、假设性提问
  如何精通诱导
  小结

[image]

上一次关于“诱导”的介绍中我们谈到了：通过不断练习，基于我们介绍的技巧，您将越来越熟练，不仅能将这一技术用于正义的目的，尤其有助于防范自己被高超的诱导者操控。

这篇文章将具体介绍：您应该如何练习以掌握这些技巧。

成为成功的诱导者需要几个关键要素：

- 不惧与他人交谈，包括处于非“常规”场景中—— 热情好客有人缘儿的形象是完全可以装出来的；

- 真心关心他人，即使是陌生人。乐于并享受倾听—— 这点很重要。真心还是假意很容易让你暴露，基本上无法伪装，你需要尝试让自己富有爱心，真的去关心他人的心情。杰出的交流者是擅长倾听的人，而不是擅长表达；

- 只在有了真正的解决方案时才提供建议或帮助。在他人说出自己的问题时，不做主观判断—— 这也很重要，资本主义原子社会中人们的同理心很差，超个人主义时代有导致人们倾向于主观意见，这会让“交流”变成自说自话，从而浪费了探索对方心理的可能性。杰出的社交工程人员绝不会看起来像一个高傲的利己主义者。

确实存在成功诱导的关键元素。美国国土安全部有一个供内部员工使用的有关诱导的小册子，这本小册子中有一些十分精彩的观点。基本上看，诱导的应用在于其有效性、很难察觉、及不具威胁性。该手册采用了“怎样避免”的角度来描述诱导，但是其后续章节中也给定了一些场景以展示其要点。你能在上面的链接中看到英文原版。

现在我们来梳理一下它提供的要点。

1.唤醒他人的自我

美国国土安全部的手册中的场景如下。

攻击者："你的工作一定很重要，某某认为你很厉害。"

目标："谢谢，谬赞了，但是我的工作并不那么重要，也就是……"

唤醒他人自我的方式简单有效，但是要注意，如果滥用这一强大的工具、或者不是出自真心，则会让目标失去热情。你不会到处和人说："哇噢，你真是全球最重要的人，长得还那么帅。"这样说只会引起别人的警觉，适得其反。

唤醒他人的自我需要微妙的处理。如果你碰到的是一个真正的自我陶醉者，在听他夸耀自己的过往成就时，眼珠不要转，不要叹气，也不要争论。微妙的自我唤醒要像这样，"你的那个研究改变了很多人在……方面的观点"；或者"我无意中听到张先生在那边说，你是他最敏锐的数据分析师"……等等。要达到目的，但不能说得太明显。

据美国国土安全部的手册介绍，精心的吹捧会促使他人说出一些从未透露过的信息，而这正是社会工程人员想要的结果。

2.表达共同的兴趣

考虑如下的模拟场景。

攻击者："哇噢，你有 ISO 9001规范数据库的背景？那么你该看看我们开发的辅助认证的报告引擎模型，我可以发给你一个副本。"

目标："太好了。我们正琢磨着在系统中添加一个报告引擎呢。"

表达共同兴趣是诱导的一个重要方面。在上面的特殊情境里，甚至比“唤醒自我”更加有效，因为它迅速拓展了关系，超越了初始交流范畴。目标同意进一步接触，同意接收攻击者发送的软件，且表达了以后继续讨论公司软件计划的兴趣。所有这些都会导致大规模安全入侵。

此时的危险在于攻击者完全掌控了形势。他控制了下面的步骤，发送什么信息、多少信息以及何时发送。对社会工程人员来说，这一步相当有利。

当然，如果是长期目标，可以找一个能共享的软件，那就更有利了。共享有用的、非恶意软件能够构建信任及和谐的关系，使目标产生进一步交流的责任感。

3.故意说错

不经意间说错一些事似乎会适得其反？不，这点如果处理得好，也能是一件利器。

攻击者：“所有人都知道 XYZ公司这方面的软件销售得最多。”

目标：“事实上并不是这样。我们公司从1998年就开始销售类似的产品了，通常我们的销售记录会超过他们的23%以上”。

再比如这样。

攻击者：“我觉得某某人他们的团队很大啊，有几百人，分布在至少三四个城市”。

目标：“这有什么，我们有一千一百人，不仅在等城市建立了根基，还正在向国家发展……”

[image]

有效使用这种方式能诱导目标说出真实的数据。

大部分人在听到错误的表达时都有一种校正的欲望，似乎他们自己的正确性受到了挑战。

人们喜欢告诉他人、显示自己的博闻强识，不能容忍错误是人类的天性。

没错，也是人性的弱点。

充分理解这一点，可以让这一攻击变得更强大。你可以通过这种方式让目标说出真实的全部细节，也能在一群人中立刻发现对这一主题最为了解的人。以便发起下一步针对性的攻击。

可怕吗？我相信99%的人都能中招。尤其是在社交网络上！想想你平时给网络上的陌生人“纠错”的冲动吧。

不过对于社交工程师来说，这种方法不宜多用，过多的使用会变假，反而引起某些人的怀疑，尤其是那些掌握了很多秘密信息的人。

他们的确有弱点，但也有着比普通人更加强烈的警惕性。他们会在下意识中犯错“说走嘴”，但不可能经常走嘴，于是作为攻击者，要见缝插针式地使用这一技巧，切勿贪婪。

4、主动提供信息

美国国土安全部的手册中对人的共性做了很好的概括。其中责任感就是一种很强大的力量。作为社交工程师，在交流中主动提供信息会迫使目标提供具有同样价值的信息。

我的一位朋友看上了一位姑娘，希望获得追求的机会。这位朋友很实在，是以结婚为目的的追求，于是很想了解下姑娘的年龄、学历等信

息。你知道的，对女士来说这些是禁忌话题，你无法直接提问。于是我建议他先介绍自己，把介绍性信息穿插在一堆其他话题之间，以掩盖目的性，并让对话环境变得自然。结果不出所料，姑娘果然主动说出了自己的年龄：“哎呀你比我大五岁呢”。很不错吧。

想试一下吗？下次在聊天中这样说，比如：“唉你听说没有啊，同事A被辞退了！现在找工作好难的，他这个年龄恐怕……真是不幸啊”。

大部分人在听到你这么说的时候都会附和一些近似的情绪，并带出近似的信息：“啊，我没听说啊！太惨了，最近很多人都遇到了麻烦，同事B正在办离婚呢，房子都保不住了”。

因为人类倾向于制造气氛和谐，表达自己的同病相怜心态，于是很多人喜欢分享类似的信息，社交工程人员可以利用这一点，为谈话设置一个基调或氛围，从而构建出责任感。

5、假装高深

看起来与上述“说错话”的装傻相反。但这是另一个强大的工具。

一般情况下，如果对方具有某方面的知识，和他讨论相关问题并无不当。攻击者可以审慎地利用这一点，首先展示一些信息，假装知道一些内情，然后使用诱导技术展开话题。过程中把别人的观点当成自己的说出来，进一步强化自己的专家假象。你笑了吗？哈哈，我知道的，我们的读者中 90% 的人在网上交流中遇到过这样的人—— 他们把自己读过的他人的观点当成是自己的观点说出来。俗称“装13”，他们应该没有恶意，但是，请注意，这种方法如果被恶意者有目的地使用，效果将非常强大。

下面举个例子。

你的任务是到一家完全不熟悉的公司谈一笔交易。你需要在前往见面之前搞明白该公司的详细信息。你发现另一些人似乎对该公司有一定了解，知道与该公司的人打交道的技巧。但是你不认识这些人。你应

该如何打探到关于该公司的细节？

以“求问”开头？再发个红包？不不，这样你不可能得到全面的真实的信息。

你可以以闲谈者的身份加入这群人的交流。首先是要基于你的目的了解到一些可以钓出有价值信息的引线知识。比如你应该对“搞关系”这个话题本身很熟悉，去找一些资料来读，记住其中的关键技巧，在和那群人闲谈中将你记下的东西随便说出来，假装自己是这方面专家。

这番发言要自然，由于话题近似肯定能引起那群人的兴趣，从而对你的发言“做出更多补充”，而这些补充就是你想要的东西了。如果你觉得信息还不够充分，那就继续使用上述以及前文中介绍过的方法，比如装傻、故意说错话等等，穿插应用它们，能更多激发目标人深入的阐述。

6、酒精的作用

这件事基本不必多说了，几乎所有人都明白它是什么意思，连秘密警察都知道邀请目标人—即被他们监视的人—吃饭喝酒，以加强诱导的可能性。所以你应该避免和心怀不轨的人一起用餐。

请注意，如果你经常在社交网络上晒高级酒品或酒局的照片，对方将能够借此了解到你的弱点！

更麻烦的是，有些时候人们并不清楚谁是心怀不轨的人，也不知道自己在攻击者眼中的价值何在。这就有些棘手了，而且很危险。有一个著名的例子能说明这个问题。

80年代，某实验室的一位资深科学家访问某国的一个研究院，举办一个关于核聚变的讲座，这是他的专业。他在核武器方面有着丰富的知识，但他也深深明白，这方面是禁区，所以需要将讲座的内容限定于他的研究主题。

讲座很成功。为他庆祝的酒会上，人们不断走上前来赞扬他的知识学术，每次都要祝酒干杯，就像你知道的那种场面。逐渐的，人们开始和他打听一些绝密的信息，例如氘和氚的点火要求，这两种元素是中子弹的组成部分。

他可没醉，他对这些问题防护得很好。但是吹捧激烈，他似乎有点架不住了，于是打算浅浅的做一个类比。于是他说，如果将这两种元素混合在一起成为一个球，从桌子上滚下来，它们就能点燃，因为它们的燃点很低。

这个看起来打趣式的无用消息实际上已经为该国的核武器研究者提供了清晰的指引。他们会以此为引线和另一位科学家交谈，然后得到更多的知识，由此类推以获得更多的知识。最终掌握了清晰的蓝图。这可是完全真实的故事。

[image]

在重要的社交工程攻击中，所有必要信息往往不会来自于同一个攻击目标，而是这样：你从第一个人口中套出关于时间地点的信息，再利用这些信息，假装是自己的了解，而从第二个人口中套出更多信息。以此类推，不断深入，最终将这些信息聚合在一起。这不是件容易事，但完全可以做到。后面还会继续分析这点。

所以为了防止被诱导，你需要记住，并不是自己感觉自己说出来的东西“无关紧要”它就真的无关紧要了，你说出的话可以作为一个引子，从而进一步对其他人使用诱导。

[image]

提问的学问

提问是一门大学问。不仅能让自己长知识，还能成为攻击的绝佳武器。

作为社交工程人员，你必需认识到，诱导绝不是走上前去问对方：“你的服务器密码是什么？”

好吧这是个玩笑。但是要知道，你的目的是利用一些琐碎的信息，然后通过它们构建出你所寻求的答案的全貌，或者通过搭梯子的形式一步步获得你想要的东西。

不论使用哪种方法，这类信息收集方式都会为社交工程人员达成目标清晰的方向。作为一个防御社交工程攻击的人，你应该有意识的去捕捉对方的话题引导是否具有台阶的效果，基于你需要保密的东西来说，这些话题是否正在打造某种路径。

好的，我们还是以攻击者的身份来演示这个问题。

下面分析较常见的几类提问方式，以及社交工程人员如何使用它们。

1、开放式问题

开放式问题就是那些无法用“是”或者“不是”来回答的问题。如果你问：“今天外面很冷，是吧？”得到的答案只能是：啊、嗯、是啊，之类的玩意。如果你的问题是：“今天外面的天气怎么样？”那么就能引导出更有效的答案，而不仅仅是“是、不是”。

这个方法不难，很多“优秀的”记者都会，尤其是那些商业媒体记者或者党刊记者，这就是为什么这里的“优秀”带有引号。它是指在社交工程学利用层面上的优秀，它本身很有心机。

想象这样一个场景。我约你见面，而临时你取消了约定，我希望知道原因。我会这样说：“你怎么了？到底出了什么事？”

“我感觉不太舒服”。

我：“啊，希望你现在感觉好一点了。哪里不舒服啊？”

这样继续下去，通过一连串的提问我就能知道为什么你没有赴约。假设我仅仅是责备，那我很可能什么信息都得不到，比如这样：“嗨伙计，你到底搞什么啊，居然放我鸽子！”

开放式问题的一个强大之处就在于，可以加入更多的为什么和怎么样。如果问题中包含为什么或怎么样，就有机会得到对方更深入的解释，其中会暴露一些你感兴趣的细节。简单说就是，让对方有机会说得更多，必然会露出线索。

2、封闭式提问

看起来封闭式提问和开放式提问截然相反啊，为什么也会有用呢？

因为封闭式提问的目的通常不是要得到详细信息，而是要对目标进行进一步的引导。

司法人员和律师经常运用这样的推理。如果想要目标遵循特定的回答路径，他们的提问往往是封闭式的，不允许答案出现天马行空的可能。比如这样：

“你认识被告人张三吗？”

“是的我认识”。

“6月9号夜晚你在ABC酒店见到了张三？”

“见到了”

“当时是什么时间？”

“晚上十一点半左右吧”

你看，所有这些提问都是封闭式的，其答案只能一两种。

[image]

激进派社区用户请从这里进入：[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

3、引导式提问

引导性提问结合了开放式和封闭式的特征，是具有答案暗示的开放性问题。比如这样："6月9号晚十一点半左右，你和张三在ABC酒店见面了，是吗？"这种类型的提问会引导对方，为其提供表达自己观点的机会，但其发挥的空间很窄。同时，引导性的问题能暗示你对答案已经有所了解了。

如果你被秘密警察做出这样的提问，要注意，他们有可能已经拿到了一些信息，这种时候你需要谨慎回答，避免被进一步套出更多信息。因为他们既然找你谈话，那就意味着他们掌握的信息至少很不充分。并且，你提供的任何信息都将被他们用来实施进一步的操控，对你、或者对更了解此事的人。

如果他们只是在宣传"我们现在什么都知道了，你要是撒谎对你可没什么好处"，等等，这种情况下说明他们根本没有了解什么关键信息，这只是恐吓，所以不用害怕，专心致志在谨慎发言的关键点上。

英国心理学家 Frederic Bartlett 总结过一个关于记忆重构的研究结果，很著名。他告诉实验对象一个故事，然后让他们立即回忆其中的部分事实，然后两周、四周之后，再次进行回忆。

Bartlett 发现，实验对象根据他们各自的文化背景、信仰和个性，修改了故事的细节，没有人可以正确的回忆完整的故事。这证明了记忆并非是对过去的正确记录，很多人会"构造记忆"来契合自己对世界的已有认知。

在被询问时，很多情况下我们的记忆库是基于自己的感知和对自己重

要的事情而形成的。正是因为这样，通过引导性问题来操纵人们的记忆是可行的。最经典的记忆操纵案例就是保罗英格拉姆案了，当事人的记忆被完全扭曲，在压力和逼问下竟然真的觉得自己就是个变态狂。

Elizabeth Loftus 是一位目击证词研究专家，也是这方面的开拓者，她曾经演示了利用引导性问题扭曲人们记忆的可能性。例如，给目标人看一张没有泰迪熊的儿童卧室照片，然后问目标人："你有没有看到一只泰迪熊在房间里？" 你并没暗示房间里有泰迪熊，所以他会按照自己的想法回答："有"还是"没有"。然而，如果提问变成这样："你看到泰迪熊了吗？"这就在暗示房间里有泰迪熊，大多数时候对方会回答"看见了"，因为人们有一种印象，即泰迪熊和儿童房间存在相关性。

并不是看起来这么简单。这样的问题往往会混在一大堆无关紧要的问题中间，过渡会非常快，如果你放松警惕就很容易中招。

反过来看，学习怎样使用引导式提问能明显增强社交工程人员收集信息的能力。

4、假设性提问

就是字面的意思—— 你假设目标人已经拥有特定的知识（对特定事件的了解）。通过假设性提问，社交工程人员能够确定目标是否真的拥有他想要的信息。

这种提问在司法调查中很常见。比如审讯者并不知道目标人是否认识张三，以及和张三的熟悉程度如何。那么这样问："张三住在哪儿？"通过目标人的回答可以分析出想要的东西。

使用假设性提问时有一点需要注意，就是：不要让目标人了解事情的全貌。这点很关键，如果目标人了解了整个意图，社交工程人员就会丧失对环境的部分控制能力，控制权会反转。并且，你也不能通过假设性问题指责目标的失误，这样会疏远目标，同样会失去控制权。

如果你是社交工程人员，在使用假设性提问时，最好已经对事实有了部分了解，然后将事实贯穿在问题中。这点非常重要！也是中国情报机构、甚至国宝会使用的方法。它唬人的效果很强大，你一害怕就输了。

假设性提问中绝不能含有虚假信息，否则目标会迅速失去兴趣，你不可能再得到真话了。并且，你必须做一个充分的前期研究，积累一些关键知识，这样就可以作出精妙的假设性提问。但请注意，如果你无法满足目标对你的知识水平的预期，反而会把整件事搞砸！所以说，要装，但不能装得太大。

回到上面的核物理学家的例子，假设我的问题是："氘和氚的温度阈值都很低，在处理它们的时候怎样避免燃烧呢？"如果我本人不是核物理学家，可能很难得到后续的内容，这样提问只会适得其反，没什么用处。你需要对假设性提问进行合理的规划，才能获得最大的效果。

警方和司法人员很擅长这手。"进去"过的人都熟悉这个，司法人员有一个"法宝"，那就是他们会这样说："在回答下一个问题之前，请考虑清楚……"。这句话给对方的暗示是：在回答时一定要诚实。这招很好用的。我们展示的是一个模式。您可别直接用原话哦，因为您没有那身制服，说出这句话很可能吓唬不了别人。

好啦差不多了，我们来总结一下。

[image]

如何精通诱导

诱导在应用中有一系列的原则，请记住以下几个要点：

- 问题太多会吓跑目标。如果你用一堆问题轰炸，不会有任何收获，只会让对方害怕。记住，对话是一种有来有往的交互，你想要提问，就需要告诉对方一些信息，这样才能让对方感觉自然。

- 问题太少也会让对方不自在。你一定碰到过那种“尴尬的沉默”，直接把天儿聊死了。这样不会有效果对吧？不要假设目标善于交谈，会长篇大论、滔滔不绝，即便真的如此也不要给TA这样的机会。你需要控制整个局面。你必须做足准备工作，针对你想要进行的话题，以便让对话有趣。

- 一次只问一个问题。我们后面会介绍“思维缓冲区溢出”，但是在这里，你的目的不是使对方溢出，而是收集信息，构建答案的轮廓。所以你必须掌握一个平衡，不能显得太急切，也不能兴味索然。

这些原则有助于你掌握这一惊人的才能。不论是用于社交工程，还是普通的学习交往的技巧，都应该遵循以下的方法：将谈话想象成一个漏斗，上面是最大的、最“中性”的部分，底部是最窄的、最直接的部分。

开始问一些相对中性的问题，通过这些问题收集一些情报线索。在对话中要你来我往，然后问一些开放性的问题。如果有需要，使用几个封闭式问题将目标引到我们最感兴趣的部分。如果情况允许，进入漏斗底部，询问最直接的问题—— 从这个漏斗中流出的就是源源不断的有价值的信息。

目前，随着冷战加深，当局对所谓“间谍”的防御兴趣加强，普通人都可能有机会直面来自国安部门的、经过高端心理训练的诱导人员。我们已经收到了类似的报告。所以，您知道这些技术的价值，它有可能事关人身安全。

小结

诱导技术是强有力的，不仅能提升社交工程攻击能力，也能提高日常沟通的水平。明白如何提供正确的节奏和方式给出恰当的问题，可以得到更多的机会。作为社交工程人员，这是一个成败的分水岭。第一印象往往取决于外表，但是，从你口中说出的话更是成败的关键。

精通诱导技术几乎可以确保社交工程人员的成功，也能为你扮演的角色大大加分。

我们上面开了一个玩笑："你没有司法部门的制服就无法使用那套原话来强迫对方说出真相"，因为不管用。其实这不仅仅是个玩笑。诱导攻击往往要结合伪装的使用，成功的伪装能极大程度上给诱导效果加分。后面我们会慢慢介绍。

[image]
[image]

什么是伪装，如何伪装，如何识破——社交工程攻防基础

[image] 关键词	社交工程
[image] 关联	[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病；[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年7月9日
[image] **Description**	心理安全；行动安全性

究竟什么是伪装？如果你有机会变成一个完全不同的人，你最想做的是什么？

- Table of Contents

伪装——社交工程学的关键基础设施
1、什么是伪装？
2、伪装的原则和计划阶段
2.1 调查越充分，成功几率越大
2.2 植入个人爱好，提高成功率
2.3 练习方言和表达方式
2.4 使用电话不会减少社交工程人员投入的精力
2.5 伪装得越简单效果越好
2.6 伪装必须显得自然
以下是一些可以让伪装更加自然的方法：
2.7 为目标提供逻辑结论或下一个安排
成功案例
小结

[image]

一名活动家被警察的卧底骗取了五年的感情和信任，这是最近公开的解密文件中曝光的惊人情节。我们都在谴责这种肆无忌惮的监视行为，但之所以它没能在短时间内被揭露，正是因为活动家的防御警惕性不充分。于是，整个故事最关键的部分之一就是本文的主题：伪装。

[image]

延伸：https://iyouport.substack.com/p/f2f?utm_source=publication-search

不必以为您自己不会遇到这种最邪恶的欺骗，也许您不是激进派，也许您对政治一窍不通，也许您真的循规蹈矩遵纪守法，但是，您依旧很有可能遭遇社交工程高手，因为您身上究竟有什么值得攻击者垂涎的价值，您自己说了不算，我说了也不算，而是取决于攻击者。

如果您已经成为政治异议、人权活动家、社会边缘群体、拥有或没有宗教信仰（这取决于不同的国家）、性认同少数群体，或者您只是被欠薪的打工族、被洗脑教育虐到发疯的学生 …… 甚至您只是希望做一点正义的事，您都应该确信自己已经成为了攻击的重点目标。

如您所知，数字监视无处不在，这是确实，但是直到目前为止 — 并且完全可以确信在未来足够长的一段时间内 — 当权者依旧会钟情于使用人力的盯防，也就是前面举出的警察卧底。因为这种方法有非常多的好处，尤其是与技术相结合使用的情况下。

于是，您完全有必要警惕身份伪装者的入侵，他们有可能就存在于你我的身边，以你我的“朋友”的身份存在于我们身边的人 — — 千万不要误会！我绝不是说鼓励您去质疑身边的朋友，绝对不是，而是希望您可以清楚地分辨恶意和善意。这是保护自己、自己的家人、自己的同伴和合作者的最佳方案。

本文主要介绍伪装的技巧 — — 即 那些渗透进反抗组织内部、异议人士身边的恶意监视者使用的方法，也是任何希望做正义的事的人免不了要使用的技巧。本文主要希望能帮您鉴别伪装者，如果您确定自己

的目的正义，您可以决定如何使用这些技巧。

[image]

伪装 —— 社交工程学的关键基础设施

什么是伪装？有人认为伪装只是社交工程过程中编造的故事或者谎言，不不，没这么简单，这是非常狭义的理解。

准确的定义应该是：以背景故事、衣着、仪表、个性和态度来塑造的角色，以完成社交工程审计工作。伪装包括你所能想到的基于对象角色的方方面面。作为社交工程师，你伪装得越全面就越令人信服。一般情况下，伪装得越简单，说明技术越娴熟。

伪装，尤其是自互联网出现以来，越来越多地被恶意利用。见下面两个真实的故事：

[image]

延伸：https://medium.com/@iyouport/%E4%BA%BA%E6%80%A7%E5%BC%B1%E7%82%B9%E8%83%BD%E6%91%A7%E6%AF%81%E4%B8%80%E5%88%87%E9%98%B2%E7%81%AB%E5%A2%99-%E7%A4%BE%E4%BA%A4%E5%B7%A5%E7%A8%8B%E6%94%BB%E5%87%BB%E5%AE%9E%E8%B7%B5-%E4%BB%A5%E5%8F%8A%E4%BD%A0%E5%BF%85%E9%A1%BB%E5%9C%A8%E4%B9%8E%E7%9A%84%E9%97%AE%E9%A2%98-1080b745430

延伸：https://steemit.com/tech/@iyouport/6bix1x

曾经一件很有名的T恤，上面写着：“互联网上，男人是男人，女人是男人，萌娃是等着抓你的 FBI 间谍”。虽然这句话有调侃的意味，但

是，事实上的确如此 — — 尤其是当我们在强调匿名安全的时候，如何分辨一个人究竟是不是他/她所声称的人，几乎是性命攸关的技能。

在互联网上，伪装技术在很多年来一直被用于黑客篡取利益，被警方和政府间谍用来抓捕诱惑他们想要的任何人。但是伪装的钓鱼方法完全不限于互联网上。

在社交工程攻击中，角色扮演或者假扮别人以达到目的，很多时候是非常必要的。世界著名的社交工程学专家 Chris Nickerson 曾经聊到了这个话题，他指出了一些要害观点。

Nickerson 说，伪装不是在扮演某个角色，或者演出某个剧情，不是让你撒谎然后不断地圆谎，而是，要你真正成为那个人。你的一丝一毫都是生活在那个人的身体内，你的走路方式、说话方式、肢体语言，与那个人一模一样。这就是关于伪装的最根本哲学。

许多人认为伪装只是乔装打扮。衣着的确能起到作用，但是，伪装这个概念本身是一门学问，作为实践者你的目的应该是完全变成另一个人。

要实现这点，社交工程人员必须明确到底什么是伪装，以作出计划，实现完美的伪装，只有这样才可以成功。

下面我们详细说明它。

1、什么是伪装？

伪装的定义是创造虚构的场景，以劝服目标受害者泄漏信息，或者作出某种行为。这绝不是仅仅说谎这么简单，很多时候它要求创造一个全新的身份，然后利用这个身份去获取信息。这是那些监视异议活动家的政府间谍最擅长的东西。

伪装没有固定的万能模式，社交工程人员必须在不同的计划中伪装成完全不同的人。

所有的伪装都有一个共同的特点，那就是：精细地研究。即：我们曾经在开源情报技巧介绍中，信息收集，和分析。这就是为什么将社交工程学、OSINT 和道德黑客，放在一起作为行动力的一部分。

伪装不仅可用于社交工程，也能在很多生活领域发挥作用。销售人员、公共演讲者、算命师傅、神经语言程序学专家、甚至是医生、律师、以及临床医学专家等，都需要一定形式的伪装，都需要创造一个适宜人们泄漏隐私信息的场景。

社交工程人员和其他伪装使用者的差异在于：对目标的设定。社交工程人员必须完全变身为伪装的角色，而不仅仅是装腔作势。

只要审计和社交工程没有结束，伪装就不能结束。很多人在退出伪装身份后很久还沉浸在原来的身份中，这说明伪装工作很到位。不过，专业伪装人员经常要使用多个在线身份、社交网络身份、电子邮件和其他账户，他们需要随时记得自己当前正处在哪个角色中。

电视台主持人是很擅长伪装的，因为他们只能透露适合发布给公众的信息。著名主持人 Tom Mischke 在这方面很在行，绝大多数观众都会自以为“了解”他，就连他的朋友也误会自己“了解”的是他本人。事实上他们只是了解了 Tom 的伪装身份。

他是如何做到这点的？

答案就是：不断的练习。

Tom 给自己安排了很多练习，对于伪装身份的站姿、说话的语气、口音、衣着、兴趣爱好……精准地掌握。如您所知，最好的也是唯一的办法就是不断地练习。这一点非常重要。

[image]

2、伪装的原则和计划阶段

像其他技术一样，伪装也有一定的原则可以遵循。下面列出了一些原则。当然这些不是全部，还可以继续添加，而这些是最为基础的，可以体现出伪装的本质：

- 调查越充分，成功的几率就越大；
- 植入个人爱好会提高成功率；
- 练习方言，或者特定的表达方式；
- 很多时候，切勿低估电话的作用，即便是在互联网时代，电话依旧非常高效；
- 伪装得越简单，成功率就越高；
- 伪装必须要自然；
- 要为目标提供逻辑结论或下一步的安排。

下面具体讨论每一条原则。（下面有一个视频，CIA前局长对伪装的分析）

https://youtu.be/JASUsVY5YJ8?si=elgXtIk6n18fwwTt

2.1 调查越充分，成功几率越大

这是不言自明的，但依旧值得多次强调。这是社交工程学的关键。

社交工程人员掌握的信息越多实现有效伪装的机会就越大。

很多时候你能感觉到，细节决定成败。

请记住：没有任何信息是“不相关”的。收集信息时要注重寻找故事、物品和个人特点，利用目标人物的性格或者情感依托，可以让你离成功更近一步。对于伪装者来说，目标才是唯一重要的事，此外一切都是为目标的积累。换句话说，他们可以做到不惜一切，可以无情无义。

[image]

延伸：https://iyouport.substack.com/p/bb3?utm_source=publication-search

恶意的社交工程人员可以不假思索地利用人们的同情心进行欺诈。911之后很多恶意攻击者利用伤亡人员为自己牟利，他们设立网站，发送邮件给目标人，并成立虚假的基金，利用人们的慈善之心骗钱。这种状况在中国应该不是新奇的。2010年的海地地震后也是这样，很多恶意的社交工程人员建立钓鱼网站，假装发布地震活动和失踪人员的信息，而这些站点利用恶意代码导致访问者的电脑被感染，进而被操控。

搜索引擎优化和市场营销专家可以在几个小时内让恶意内容处于搜索功能的首页位置。提升搜索排名并不是什么高难技术，百度那种虚假广告占据首页的状况，其实一点都不奇怪。想在谷歌中排名前位吗？你只需要请一位社交工程师，他们一般都深悟市场营销伎俩。

2.2 植入个人爱好，提高成功率

通过个人爱好提高社交工程的成功率听起来很天真，但是有助于让目标信服你。

不过请注意，如果你在一开始声称自己很擅长某方面，但随着时间推移显示出你并不擅长，那么这绝对是毁掉信任最快速的方式了。作为一名社交工程人员，如果你从没见过服务器机房，没有亲手拆过电

脑，那么就千万不要伪装成技术人士，绝对会失败。

伪装中加入自己感兴趣的话题和活动，从而能侃侃而谈，这会让你显得聪明而自信。

自信有助于说服目标你就是你宣称的那个人。你的伪装身份必须有更多的知识保证，以令人信服。其实不是很难，有些时候你只需要通读几本书就够用。

对于社交工程人员来说，获取知识、研究感兴趣的话题，这是非常重要的。在伪装时，你可以聊故事、观点和工作，也可以聊你很了解的某种兴趣爱好，或者一些谈起来很舒服的话题，这样都能奏效。如果你像在互联网上那样只为了证明自己的“是对的”，肯定做不成社交工程工作。

Stevens 博士曾经的警告依旧非常重要：“记住，你的自信心始终与任务和自身处境密切相关。不同情况下，我们的自信心是不一样的”。这句话很关键 — — 因为自信心直接跟别人如何看待你这个人有很大关系。自信 — 而不是自傲 — 可以更容易建立信任和默契，而且可以让人感觉放松。尽量让目标谈论你感觉舒服的话题，然后你就可以自信地发挥了。这很重要哦。

1957年，Leon Feastinger 提出了认知失调理论。该理论认为，人们倾向于协调自己的信仰、观点、乃至几乎所有的认知。如果态度和行为之间存在不协调，那就必须要修正这种不协调。

Feastinger 博士提出有两个因素会影响这种不协调的强度：

- 不协调的信念的数量；
- 每个信念的重要性。

随后他提出了三种可以消除这种不协调的方法 — — 每一位希望使用社交工程技术的人都应该高度重视以下这三点：

- 降低不协调信念的重要性；
- 增加更多的协调信念以超过那些不协调的信念；
- 改变那些不协调的信念以使它们协调。

这些真的非常重要！如何利用这些提示？当伪装的角色需要你表现自信的时候，如果你不够自信，就会不协调。这些不协调会引发各种红色警告，给你们之间的默契、互信和下一步进展带来巨大的阻碍。会直接导致你失败。

记住，你只有一次失败机会。第一次出错就是最后一次出错。

避免这种悲剧收尾的最好办法就是，加入更多的协调信念以使其数量超过那些不协调的。想想看，目标对你的伪装期待是什么？了解这些可以让你的行动、谈吐、和态度等方面更好地迎合目标人物的思维和情感，从而在你们之间构建起信念系统，让对方忽略掉那些值得怀疑的东西 — — 渗透入反抗组织内部的当局线人非常擅长这些操作。

一个技术娴熟的社交工程人员同样可以将不协调的信念变成协调的。虽然这很棘手，但是，这项强大的技巧非常值得拥有。也有可能你的伪装和目标的构想不一致。你可以回想一下《Doogie Howser, M.D》，豪斯医生很年轻，这和角色设定的顶级医生似乎不相符，这是一个不协调的信念，但是，他的知识和行为又可以让“目标”觉得那是协调的。社交工程人员完全可以通过观点、行动、尤其是知识，让他的伪装和目标的认知达成一致。

伪装的方法有很多，成功的关键在于：明智地选择适合你的那一种。

2.3 练习方言和表达方式

我的一位老师是方言专家，他最大的魅力就是，不论任何人，只要报

出自己的家乡，他立刻就能使用当地的方言和对方寒暄。

这的确是一种非凡的魅力。如果你试过就会知道，绝大多数时候对方会立刻喜欢上你。如果你是社交工程人员，熟练掌握方言就能够帮助你更快速地和目标人建立互信关系。

这也许需要花费很多精力，但是如果能学好，它将非常有帮助。如果学不好也没关系，那就使用你最擅长的语言，努力让你的语言富有魅力，可以达到一样的结果。

当然，作为社交工程人员，你最好能掌握至少一种方言。

2.4 使用电话不会减少社交工程人员投入的精力

最近几年，互联网开始主导某些“不需要面对面交流”的社交工程活动，就像美国警察在 Facebook 上伪装身份钓鱼黑人活动家所做的那样。然而在过去，电话是社交工程中最不可或缺的一部分。由于互联网的出现，很多社交工程人员开始不注重电话的强大能力了，这其实是一种失败。

这里想说的是，电话依然是一种强大的社交工程利器，不该因为互联网的非人格化性质而减少对它的使用。

很多时候，社交工程人员在策划电话攻击时的想法会有所不同，因为利用互联网看起来更简单一些。但是要记住，使用电话进行社交工程时需要投入同等的精力、同等深度的研究和信息搜集，最重要的是同等水平的练习。

你必须研究一种最佳的模式，从语速到语调到音调，以及措辞，要让所有的细节都为了你的目的服务。要时刻记住你就是你伪装的那个人，而不是你在伪装 —— 这很重要。除非是精神病患者，我们每个人在撒谎的时候都会不由自主地紧张，而当你深信自己就是自己的角

色时，这种紧张感就能消失，否则会导致你失败。

这里也要强调合作的重要性。你最好能和一个小组协作练习，他人能比我们自己更容易观察到我们自己哪里出错，哪里不协调，更容易指出我们的纰漏。并且你应该有一个尽可能完善的剧本大纲，让自己深深融入这个大纲之中，把自己变成主角。

是剧本大纲，而不是剧本，这非常关键，它应该在全部细节上都满足于你的目标，还要尽可能推测到对方的不同反应，为每一种反应想到理想的回应方式。设想这样一种场景：你不得不打电话给一家公司或一个机构，因为他们搞错了一个订单，或者服务有问题。你非常生气，打电话就是为了抱怨的。当你和客服解释了之后，不管你有多失望，客服都没有为你提供任何帮助，她只是在说："本公司承诺提供最好的服务，请问还有什么需要帮助的吗？"……你会知道这有多傻，对吧。这就是由于该客服只有剧本，而不是大纲的结果 —— 它是死板的，而灵活性必须是社交工程的要素。

使用电话提高伪装的可信度，是得到目标认可的最快捷方法之一。电话允许社交工程人员去哄骗或者假冒任何事。

比如这样的例子。我现在需要假设自己正在一个忙碌的办公室里给你打电话，我如何才能制造出"忙碌办公室"的虚假氛围？很简单，去录制一个音频，放在电话旁，你需要作出身处忙碌办公室的人特有的快语速，配合背景音，效果会非常逼真。

伪造电话号码欺骗要相对容易一些。像 www.spoofcard.com 等服务或者自制一些办法，都可以帮助社交工程人员改变来电显示的号码，对方会认为你就是从某个声称的公司内部、白宫、CIA、警察局、或者当地银行打来的电话。

[image]

2.5 伪装得越简单效果越好

越简单效果越好，这一点都不夸张。如果伪装有错综复杂的细节，以

至于忘记了任何一个细节都会导致失败，那么就真的会失败了。保持故事情节、事实和细节的简单性。就能增强可信性。

人际欺骗领域最有名的心理学家和研究人士 Paul Ekman 博士曾经发表了一篇文章题为《失败的谎言》，其中写道：

> 很多时候你没有时间去准备，进行练习和记忆。就算事前有充分的预案，也有可能突然冒出一个不能预见的方向。你可能很聪明，但是也很难预见所有可能被问到的问题，于是很难预备所有答案。光有聪明的头脑是不行的。而且，即使不是为情势所迫改变方向，某些撒谎者也会由于记忆问题而想不起前面的描述，结果就不能快速解答新的问题。

这个重要的观点将为什么越简单越好，解释得非常清楚。如果伪装得很复杂，努力去记住所有内容几乎是不可能的，一个很小的错误就能毁掉你的全部。

你必须记住一切事实，并且不要过分追求细枝末节。一个简单的伪装允许故事发展，并且允许目标运用想象去填满那些空隙。切勿试图将伪装做得很精致，但必须牢记伪装中的关键细节。

并且——这里提到过那个方法——专业的罪犯和骗子们会使用一些伎俩，包括故意出错。这个想法是基于“人无完人”而建立的，一些小错误会让人感觉你更真实。如果运用这个策略，就必须留心你决定去犯的那些错误，虽然这确实能使对话更自然，但是也增加了伪装的复杂性。还是建议少用这一花招，如果有必要使用，要让它尽可能简单。

2.6 伪装必须显得自然

要想让伪装显得自然，就需要使用如前文中强调的大纲模式，而不是剧本模式。大纲模式下社交工程人员可以自由地发挥，使用太详细的剧本会让你变得很机械。

伪装中可以加入社交工程人员感兴趣的项目或故事。如果每次有人问一个问题或者做出一个论述，你都支支吾吾，需要深入的思考，而不能立即做出明智的回答，你的可信性就会大打折扣。

以下是一些可以让伪装更加自然的方法：

○ 不要考虑自己的感受：这点很重要。因为通常在伪装时如果想太多就会融入更多的个人情绪，然后恐惧、不安或焦虑就会随之而来，这些都可能导致失败。另外你可能不会经历不安和焦虑，但有可能过度兴奋，这同样会导致你犯很多错误。

○ 不要把事情太当真：当然，在生活中这就是一条好建议，而且非常适用于社交工程。作为一名专业的安全人员，你有一份严肃的工作，这是一件严肃的事，但是如果不能笑对自己的错误，就可能会沉默不语，或者在处理后续的小事时如临大敌。我绝不是建议你视安全如儿戏，但是如果你将潜在的失败当作人生中的重大失败，那么产生的压力肯定会导致更坏的结果。只有正确地看待小的失误，才能获得更大的成功。

○ 学会找到相关信息：即 摆脱思维的束缚，融入这个世界。这是一个非常棒的建议。社交工程人员可能全力计划好了前三个步骤，但是却遗忘了这个关键细节，就有可能会使伪装土崩瓦解。要始终留意身边出现的信息和状况，包括目标的肢体语言、说的话、微表情等，将其应用到自己的行动中。

同时，记住说话者能看出什么时候你没有在认真听他说话。这会让很多人感到不爽。每个人都经历过自己的话被别人当耳旁风，你能记得当时自己的感受。也许他们有各自的理由开小差，但这样做的确是非常扫兴的。

一定要注意听目标说的话，集中注意力，你会听到一些对他们很重要的细节，同时也能够获取有助于自身取得成功的信息。

○ 争取多积累经验。毫无疑问：多多练习。通过实践去积累经验，要做到能成就伪装，也能识破伪装。抛开死缠烂打的方式，与他人展

开简短的会话，可以使你在伪装的时候表现得更加自然。

这些方法绝对能使社交工程人员在伪装中占据优势地位，具备自然的伪装能力可能是一种天赋，但是练习和充分的准备完全可以让没有天赋的人也能做到最好。

[image]

2.7 为目标提供逻辑结论或下一个安排

不论你是否相信，事实上，人们都希望被告知下一步该做什么。想象一下，你去看病，医生给你做了检查，并且在纸上记录了一些东西，然后告诉你："好了，下个月见"。这是让人无法接受的。就算是听到坏消息，人们也希望被告知下一步该做什么。

作为社交工程人员，你要离开目标时，可能需要他采取或不采取行动，或者你已经得到了想要的，只需要离开即可。不论是怎样，这个时候都不能立即离开，你应该给目标一个清晰的结论，否则很可能会令目标怀疑你的目的。

就像医生做完检查却不给你指示，直接打发你回家那样，如果你是社交工程人员，伪装成技术人员进入一栋大楼，在复制好自己想要的文件后一句话不说就走了，肯定会让人怀疑你。甚至有人会立即给你伪装的技术公司打电话，询问究竟是怎么回事，你就露馅了。

你必须做一些总结，哪怕很简单也行，要像专业人士那样阐述："我已经检查了服务器，并修复了文件系统，你们会发现系统在未来几天里运行速度提高22%"，目标就会感觉"花钱值得"。

还要注意的是，你选择的伪装身份必须和你提出的所有请求相一致。如果你伪装成技术人员，就不应该命令周围人做或者不做什么，因为你在为他们服务；如果你伪装成UPS快递员，就不应该要求进入机房。

就如以前提到的，一次完美的伪装需要很多步骤。但对于希望进行完

全可信的伪装的社交工程人员来说，这两篇文章中的内容已经足够您使用了。

成功案例

美国历史上最大的银行抢劫案 — — Stanley Mark Rifkin 亲手策划，没有花一分钱、没有使用任何武器、没有任何人质，他一个人轻松带走了1020万美元。

Stanley 是一名电脑极客，在他的小公寓里开了一家电脑咨询公司，他的一个客户是给美国证券太平洋银行提供电脑服务的公司。坐落在洛杉矶的美国证券太平洋银行总部有55层，看上去就像一个花岗岩和玻璃组成的堡垒。身穿深色制服的保安人员在大厅里巡视，隐形的摄像头监视着所有来访者的一举一动。

这栋大楼看起来无懈可击。那么 Stanley 是如何轻松拿走了这么多钱的？

银行的电汇机制应该是最安全的，每笔电汇都必须输入密码，而且这个密码每天都会被强制修改，只有特定的人才能知道。密码被贴在安全房间的墙壁上，而且只有特定人员才可以进入这个房间。以下是公开资料的描述：

> "Stanley 来到美国证券太平洋银行，那里的人理所当然地认为他是计算机工作人员。他乘坐电梯来到电汇室所在的D层，伪装成友好而且和蔼可亲的年轻人，他竟然进入了贴着密码的那个房间……他记住了密码，然后在没人怀疑的情况下离开了。然后电汇室的员工接到了麦克汉森的电话，他自称是该银行国际分部的员工，他正确地给出了当天的密码，要求为纽约欧文信托公司资金账户进行转账。整个过程没有任何怀疑。但事实上，那个麦克汉森就是 Stanley。他取走了1020万美元。"

但这显然是太粗略的描述，完全无法体现其中社交工程学的要点。让我们梳理一下：

- 为了能够在密码房间里不引起怀疑，他需要足够的自信和镇定；

- 提出汇款要求，他需要一个足够令人信服的故事，而且需要考虑足够多的细节来自圆其说；

- 面对可能出现的问题，他必须表现得足够自然；

- 为了不引起银行员工的怀疑，他的所有表达都需要足够熟练和流利……

这些伪装必须经过细致的安排，要考虑到每一个极其微小的细节。直到遇见了一个前同事，Stanley 才被揭穿。Stanley 被抓的时候，认识他的人都非常震惊，甚至有人强调：“他不可能是小偷！人人都喜欢Mark！”

很显然，他的伪装是非常到位的。他的计划经过了深思熟虑，安排周详，排练娴熟。他知道自己的目标是什么，每一步都做得非常完美。如果不是很早以前熟悉 Stanley 的人看了新闻后把他认了出来，他是不可能被发现的。

Stanley 的计划是把偷出来的钱变成不可追溯的钻石。为了实现这一目标，他首先需要变身一名银行雇员以拿到钱，然后变身一名钻石收购商将这些现金“洗掉”，最后把钻石卖掉，获得可以使用的、无迹可寻的、干净的现金。

他的伪装不涉及装备和说话方式的变化，却需要依次扮演银行工作人员、钻石采购商和销售商。这其中需要完成3到4次、甚至5次身份转化，他做得非常完美，几乎骗了所有人。

小结

伪装通常是专业身份窃贼开始入手的第一步。鉴于身份盗用最近几年来已经越来越频繁地出现，你真的有必要知道它的原理，以便做到精准有效地识别。

异议人士中经常出现抓特务的游戏，因为人们意识到当局派来的卧底会潜伏在自己的队伍中。这种警惕性是必要的，但是，如果你使用了不专业不靠谱的鉴别方式，其结果不仅是无法发觉真正的的卧底，更会严重损伤团队内部的互信。得不偿失。当局毫不忌讳宣传他们的群众斗群众策略，就是希望为异议群体制造混乱和恐慌，如果你不能精准识别并引发了内部失信，那就彻底中计了。

建议返回本文标题下的“关联”栏目，进入两个相关专题：反渗透，和反侦察。

尤其是在互联网上的卧底，也许会感觉很难识别，但是这种手段却非常常用，就如前文所介绍的，美国警方假冒活动家潜入社运组织内部钓鱼，事实上匿名者组织也被这样渗透过。但是我们不能因此放弃利用互联网的动员和联合，否则将是因噎废食。

对于中国的反渗透工作来说，鉴别应该不是很难，但是肯定需要时间和精力。此处不方便太多说明，原因很简单，当局也在关注着这些公开发表的内容，一旦写明，其方法立刻就会失效，因为对手会迅速调整策略，以防止自己被发现。于是，如果您对此感兴趣，请努力研究，根据我们提供的社交工程基本知识，结合您的经验，完全可以总结出一套自己的鉴别方法。

伪装的知识并非只提供给防御，它也可以用来作为技巧去追求正义的目标。反抗需要很多技巧，从在线到线下，从数字技术到心理学和社会学，掌握得越多您的行动就会越顺利和安全。最后，还是那句话：重在练习。

[image]
👄

套话：5种有效的社交工程启发术

[image] 关键词	社交工程
[image] 关联	👄语言是强大的武器 - 如何使用它？人性黑客：致命的诱导
[image] 创建时间	2025年7月10日
[image] Description	心理安全

根据 FBI 的定义，“启发”是一种可以有效钓取情报的技术。

换言之，“启发”是一种看似随意对话的战术，用于从目标人口中提取信息，而不会让对方感觉到自己正在被询问，不会感觉到任何压力。

这是个技术活。因为稍不留神就可能引起目标人的警惕，对方就会碍于很多想象中的危险而拒绝进一步交流。

社交工程师使用“启发”的技术收集有价值的信息，然后在开展更大规模的攻击中有效地使用它们。

我们下面来介绍一些社交工程师的小把戏。

[image]

1、奉承

不是拍马屁哦！奉承是门学问，你需要做到调动目标人的自豪感，并且同时，丝毫不会显露你的目的，它看起来就像是一种极为普通的描述和无心的闲谈。

吹牛不论是在东方还是西方都是不受欢迎的。人们常常会为自己的成就而感到骄傲，但是由于这份传统的耻辱感而找不到分享这些成就的机会。而当你称赞一个人时，它通常会自然而然地打开对方吹牛欲望的大门。真话就会漏出来。

例如，如果你真情实意地赞美对方，他们可能就会感到不得不详细说明自己参与的项目。即使目标人正在推让以示谦虚，他们也会下意识地主动谈论你发起的主题并很可能放弃信息的保密性。

一个优秀的社交工程师应该可以通过深入挖掘这些人类的潜意识来利用这个机会。

值得一提的是，即便你描述得有点夸大也很少会引发反击。你可以完全打开目标人的话匣子。一个健谈的目标可以成为社交工程师的信息金矿。

而另一方面，需要注意的是，如果你在提到目标的衣服或亲友时采取夸张的奉承，很可能是灾难性的！这种方法必须用机智来处理。性骚扰或临界骚扰声明绝不应成为社交工程计划的一部分。因此，应该不惜一切代价避免它。

相反，应该将恭维从个人特征和外观转向更多物质性的事物，例如，鞋子、手表、公文包、眼镜、皮夹，简单说就是你不应该评论目标人本身，而是要抓住目标人拥有的东西去赞美，不论是能力还是物质品味，不论是眼光还是理想计划。

2、虚假陈述

这种策略涉及故意的虚假陈述，希望目标能够用准确的信息来纠正你— — 很多人都有显摆自己“知识”的倾向性，当听到错误的描述时他们往往坐不住，想要立即纠正你。

[image]

返回：👄语言是强大的武器 - 如何使用它？人性黑客：致命的诱导

举个例子："我听说他们的大厅里有十七个摄像头，十二个警卫，还有指纹扫描仪。他们说那个地方就像诺克斯堡！没人能进得去。" —— 这种策略的关键是要包含细节并大大地夸大场景。在此情况下你的目的是了解大厅中究竟有多少个摄像头，所以，请务必夸大数字。

不要简单地说大厅里有几个摄像头。你的目的是让目标人通过陈述正确的数字来纠正你。如果有人正在宣讲不正确的信息，例如摄像机的数量，那么当其他人知道无可否认的真相时，纠偏的那一部分人性就会被调动起来。

人类的行为特征是该策略的核心，也正是我们想要抓取的。

值得一提的是，如果虚假陈述太接近现实，那么目标就可能觉得没有义务纠正你。关键是要夸大细节，以便刺激目标感觉有必要纠正你的描述。

3、人工无知

如前所述，虚假和夸张的陈述对人类行为能起到明显的刺激作用，引发纠正错误陈述的反应。以同样的方式，人类具有教导和教育他人的内在愿望。于是，社交工程师经常使用人工无知来假装自己对某个主题缺乏经验，以便激发目标教育别人的欲望。

举个例子比如这样，"我对运动探测器一无所知，但我敢打赌警察经常使用这种东西。我听说他们连落叶都能准确探测到，好可怕。"

教导别人的内在欲望尤其值得注意，你要利用那些对目标来说具有亲和力的主题，就能增加他或她将被迫教育你的机会 —— 还是我们曾经一直强调的：你需要首先了解你的目标人，了解他们知道些什么、对什么感兴趣。

融合上述的"启发"策略会能增加成功的机会。根据经验，结合奉承战

术和人工无知已被证明是非常有效的。两者作为启发策略可以非常好地相互配合。

提升自我可以让人们更容易打开话匣子。一个健谈的目标对于社交工程来说是一个极好的目标 —— 你说得越多，泄漏的东西就越多。这种方法还可以在社交工程师和目标之间创造一种相似性 —— 而相似性是影响他人的最有力工具。

4. 共情

不是一般的那种自然的共情，这里所说的共情是一种策略，因为它是假的，是故意制造出来的气氛。

这种策略利用人类倾向于吹嘘或抱怨自己的感受。

当一个人将自己的感受传达给另一个人时、甚至是完美的陌生人时，就会借助情绪创建出极为亲密的心理关系。因此，他或她可能会因此放弃更多信息，被社交工程师所利用。

成功利用共情策略的关键是要专心，耐心地倾听并共鸣目标人的感受。

这是一个常用的探测人性的策略。一个优秀的社交工程师完全可以为目标人的吹嘘或抱怨创造一个“安全”的环境。一种方法就是表达体察目标人的所有感受，无论是积极的还是消极的。这便可以在社交工程师和目标人之间建立心理联系。社交工程师将自己描绘成一个永远不会再见面的人 — 也就是一个私密的树洞，就能创造这种安全的环境。

结果就是，它减少了目标对陌生人的否定判断的可能性，反过来又增加了目标额外的披露信息的机会。从本质上讲，它发出一个信号，表明没有“无论你说什么，离开这张桌子后就没有任何人再记得这些”。

这一战术的根源是首先做一个出色的倾听者。这说起来容易，但是做

起来很难。社交工程师必须经常采取肢体语言进行眼神接触，通过心理暗示强调“我能深刻地理解你的感受，我们在一起很安全“。

其次，表达同意目标的想法、并通过分享您自己的类似经历经验，都可以加强目标继续畅谈的信心。

5. 勾子

社交工程师使用这种策略是为了从目标获取更精确的信息。为了实现这一点，社交工程师会给出非常高或非常低的近似值，以试图诱使目标人用更具体的数字作出响应。

例如，如果这场行动的目的是了解大厅内布设的运动检测器的数量。社交工程师可能会对目标这样说：“我猜他们在安保工作方面很警惕。大厅里最多有五个动作探测器吧。“ 事实上有30个。

因为我们遇到的大多数保安人员都喜欢抱怨或吹嘘他们自己所保护的环境，而他们中的大多数人都倾向于对他们所保护的环境感到自豪。因此，他们喜欢谈论相关安全性的问题 — — 这就是一个勾子。

如果你的目的是要了解作为安全防护装置的运动探测器的数量，那么调动安保人员的自负就是一个捷径 — — 你可以故意低估运动检测器的数量，这样就能触发他们的骄傲以纠正你！既然你已经牵引住了对方的自我，下一步就可以利用“启发”术来让他们进一步多说。

[image]

好啦。需要说明，以上绝不是全部！它们只是最常用的一些策略，需要通过更多的练习以获得经验，从而摸索出其他实战技巧。

提供这些知识是在支持正义的行动者，而不是培养狡诈的骗子。

[image]

夺回你的思想：宣言

[image] 关键词	
[image] 关联	[image]S08精神心理安全-总章节：唤回心灵
[image] 创建时间	2025年12月20日
[image] **Description**	自我照护和互助；心理安全

[image]

[image]

建设中！敬请期待。

[image]
[image]

[image]

关键词

[image] 心理安全

Description

[image]

组织、照护和互助 - **Organizing&SelfCare&MutualAid**

一个不爱你的人什么都能做得出来。或者说，他们对你做出什么都不会令人惊讶。 我们需要彼此间的爱才能实现互相信任和依赖，才能做到危难之时彼此照应相依为命。 不论你为自己打造多大的“可利用价值”都不足以给你这样的安全感，相反，那只会让你始终处于随时可能被取代的恐慌中。 只有爱，才是无可取代的。 人不是工具，我们不是彼此的玩偶，这是我们的组织结构区别于全球资本主义社会大环境的根本。

[image]
[image]

设备好像被黑了怎么办？ - 数字急救包

[image] 关键词	个人 互助 恶意软件 电脑 移动设备
[image] 关联	工具-Tools ；[image]恶意女仆和查抄 ；[image]防篡改准备 ；[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08 ；[image]数字技术限制和最佳实践
[image] 创建时间	2018年7月10日
[image] **Description**	自我照护和互助；操作安全性

找对了帮手，是解决问题的最重要一步。

- Table of Contents

安全通信
寻求并提供远程帮助
1.
2.
帐户劫持
缓解问题的第一步：
步骤1：
步骤2：
步骤3：
步骤4：
步骤5：
如果您无法再访问该帐户：
设备被抢占
首先回答一些简单的问题：

该设备有哪些安全保护？
设备上有什么？
缓解问题
第1步：
第2步：
第3步：
第4步：
如果您找回了设备
恶意软件
如果您怀疑设备上存在恶意软件感染，您可以执行以下操作。
缓解问题
‘清洁’您的设备
反病毒
DDoS 缓解
首先回答一些简单的问题：
诊断信息

[image]

软件只能起到一半作用，操作安全是至关重要的。

普通用户的不小心最多是搞坏设备、被盗取私人信息（虽然这已经够呛了），如果您是敏感人士，不小心会导致您入狱，甚至牵涉到一群朋友的人身安全（不要和那些不重视安全问题的人走得太近）。

但万一真的中招了，怎么办？这里推荐一个急救工具箱，希望能有更多人学会使用它。

[image]

“数字急救包” 旨在帮助面临常见类型数字威胁的人提供初步支持。

这一套件为面临攻击的人权维护者、博主、活动家和记者提供了一套自我诊断工具，

并为数字急救人员提供指导，以帮助受到威胁的人。

当您或某个联系人面临数字威胁并希望寻求支持时，该工具包首先会建立安全通信的方式。然后继续探讨有关帐户劫持、设备查封、恶意软件感染和 DDoS 攻击的部分。

每个部分都以一系列有关您、您的设备和您的情况的问题开头。这些问题将指导您进行自我评估、或帮助第一响应者更好地了解您所面临的困境。然后，它列出了理解并可能解决问题的初始步骤。这些步骤还应该帮助您或第一响应者识别何时应该向专家请求帮助。

数字急救包并不是所有数字紧急情况的终极解决方案。但它致力于为您提供工具，帮助您首先评估正在发生的事，并确定您是否可以自行缓解难题。如果您对实施此处列出的解决方案感到不安或不确定，请向经过培训的专业人员寻求帮助。

数字急救套件的灵感来自于：每个人都有能力采取预防措施，每个人都有能力帮助面临麻烦的同事和朋友。该套件的自我诊断质量还应使记者、博主、活动家和人权维护者能够了解他们的数字资产发生了什么，能够更快地确定何时应该寻求帮助，他们有什么样的帮助需要，并提高个人数字安全性。该工具包可以将那些最可能受到数字攻击的人列入第一响应者清单，也就是您可以更便利地获得支援。

数字急救工具包是 EFF, Global Voices , Hivos & the Digital Defenders Partnership , Front Line Defenders , Internews , Freedom House, Access , Qurium , CIRCL , IWPR , Open Technology Fund 和个人安全专家的共同努力（这些都是数字安全领域的国际知名组织，您很容易搜到关于他们的介绍）。数字安全和快速反应领域是一项正在进行中的工作，如果您是技术人员，想要添加内容、或者发表评论或提出问题，请访问 Github。

[image]

安全通信

[image]

返回：激进社区用户请从这里进入：[image]数字技术限制和最佳实

践

本部分将为您提供有关在面临潜在数字攻击而寻求帮助时建立安全通信的方法的指导。

作为一般规则，重要的是要了解大多数“常规”通信工具都是不安全的。移动和固定电话通信不加密，可被政府、执法机构或其他拥有必要技术设备的人员窃听。发送未加密的通信就像发送明信片一样，任何有权访问明信片的人都可以阅读消息。

安全通信始终是安全性和便利性之间的权衡。选择最合适的安全通信形式取决于您的独特情况，威胁模型以及您参与的活动。Digital First Aid Kit 专门针对那些受到数字攻击的人，因此此处会假设您处于高风险之中。

[image]

返回：[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

最后，在沟通时有不同的安全级别。

提供端到端加密的通信工具（如 PGP 加密的电子邮件，或在手机上使用 OTR 或 Textsecure 或 signal 聊天）是推荐的，那些传输层加密工具（如 Gmail，Facebook 或 Twitter）不安全，不该推荐。未加密的通信（如明信片，手机或短信）最好不要用。

希望您利用现有的资源和技能，尽力做到最好。

寻求并提供远程帮助

当您从第三方寻求远程帮助时，请记住以下几点：

1.

如果您认为您的某个设备或帐户出现了问题，并且您对下一步该做什么感到不确定，请向您认为可以信任的经过培训的技术专业人员或（国际）国家组织寻求帮助。

请不要依赖您在网上找到的不明身份的人。

以下是您可以联系到的组织：

- EFF： eff.org
- 前线防御者：frontlinedefenders.org
- CPJ：cpj.org
- RSF： rsf.org
- Accessnow：accessnow.org
- 数字捍卫者： hivos.org
- 自由之家：https://freedomhouse.org/
- Internews：https://internews.org/
- IWPR：https://cyber-arabs.com/

2.

在寻求帮助时，还要记住您使用的设备可能是有计划攻击的对象。为了与可以帮助您的人建立安全的通信线路，需要通过备用的值得信赖的设备与他们联系。

[image]

帐户劫持

您在访问电子邮件、社交媒体或网络帐户时遇到问题吗？帐户是否显示您无法识别的活动？您可以采取许多措施来缓解此问题。

首先回答一些简单的问题，如下：

- 您遇到哪些服务有问题？
- 您是唯一使用该帐户的人吗？（有时，也许您团队中的多名成员都可以访问 Facebook 群组页面，WordPress 博客或电子邮件帐户）。如果有多人可访问此帐户，请首先检查您的朋友或同事是否更改了权限。
- 用户名和帐户的 URL 是什么？
- 您无法访问自己的帐户吗？
- 您能看到其他人使用您的账户吗？
- 您收到过警报或有朋友/联系人收到似乎来自您的奇怪消息吗？
- 您在这个问题上看到了什么其他证据？

缓解问题的第一步：

如果您仍然可以访问该帐户，请移动到另一台计算机 — 您认为安全的计算机。

登录并更改您帐户的密码。

然后转到以下步骤：

步骤1：

停止使用此帐户进行敏感信息的交换，直到您更好地了解情况为止。

步骤2：

如果可能，请查看连接历史记录/帐户活动（Facebook，Gmail 和其他电子邮件平台的可用功能）。检查您的帐户是否在您不在线期间被使用过，或者是否从不熟悉的位置或 IP 地址访问过。

步骤3：

查看帐户设置。设置被改变了吗？对于电子邮件帐户，请检查电子邮件中的自动转发，电话号码备份/重置电子邮件地址，与不同设备（包括电话、计算机或平板电脑）的同步，应用程序权限或其他帐户权限。

步骤4：

更改链接到此帐户的所有其他在线帐户的密码。例如，如果您正在查看电子邮件帐户，并且该帐户是另一个帐户的恢复地址，那么请立即更改该帐户的密码。

步骤5：

不要停在这里，请按照以下重要步骤操作。

如果您无法再访问该帐户：

遵循不同提供商的恢复程序。

请注意，不同的服务有不同的方法来重置您帐户的密码。有些服务会使用您的辅助邮箱地址向您发送更改密码的链接，而其他的会将其重置为上一个密码。

在重置案例中，重新获得帐户访问权限后立即更改密码非常重要。如果这些步骤不起作用且您的帐户被滥用，请与上面列出的某个组织联系，以获取关闭帐户的支持。

设备被抢占

你的设备丢了吗？是否被第三方窃取了？或者被警方扣押了？在任何这些事件中，非常重要的是要清楚地了解发生的事，可能导致哪些类型的数据和帐户容易受到攻击，以及必须采取哪些措施来防止泄露和滥用您的信息、联系人和帐户。

首先回答一些简单的问题：

- 发生了什么？
- 丢的是什么样的设备？电脑，手机，平板电脑还是外接硬盘？
- 您何时何地丢失了该设备？

- 怎么丢失这个设备的？被另一个人偷走了，还是被国家当局占用了？或者只是忘记放哪儿了？

该设备有哪些安全保护？

- 设备是否受密码或其他安全措施保护？
- 设备上运行的是哪个操作系统？这是合法版本吗，还是非法的，越狱的或 root 版？
- 设备是否已打开完整磁盘加密？
- 丢失时设备处于什么状态？登录了吗？设备是否打开但密码已锁定？是睡眠还是锁屏？或者完全关机？
- 您是否可以远程访问设备？

设备上有什么？

- 清点设备上的不同类型的敏感信息。示例包括电子邮件，聊天记录，社交媒体，联系人（电子邮件，聊天软件等），文件，位置数据，信用卡数据等。
- 它使用什么样的基础软件，即 Windows，OS X，Android，iPhone？
- 您是否使用加密工具进行电子邮件或聊天（例如 PGP 或 OTR）？
- 该设备可以访问哪些帐户？包括设备可以访问的电子邮件，社交媒体，聊天，即时消息和银行帐户，已将密码保存到帐户的浏览器，可显示您的互联网浏览历史记录的 Cookie，身份验证

令牌（如 iPhone 上的指纹解锁），以及使用该设备的帐户用于二次认证的功能。

- 您的帐户是否已保存密码和/或自动登录？这在电子邮件，Skype和其他聊天程序中很常见，或者如果您将密码保存在了 Web 浏览器中而不是像 KeePass 这样的密码管理器中？

缓解问题

如果您的设备仍然丢失或被第三方占用无法收回，则首先要采取的步骤如下：

第1步：

对于该设备可以访问的所有帐户（电子邮件，社交媒体或任何网络帐户），为所有这些帐户删除此设备的授权。这可以通过在线转到您的帐户并更改帐户权限来完成。

第2步：

更改此设备可访问的所有帐户的密码。

第3步：

为此设备可访问的所有帐户启用两步身份验证。

请注意，并非所有帐户都支持2FA。不支持的最好放弃它。

第4步：

如果您在丢失的设备上安装了工具，可以删除设备的数据和历史记录，请离开使用它。

如果您找回了设备

如果您已经取回了设备，请小心！因为您不知道谁动过它。根据您所面临的风险级别，您应该将该设备视为现在不受信任或受到损害。

问自己以下问题并评估设备遭到入侵的风险：

- 该设备离开您的时间有多长？
- 谁有可能获得它？
- 他们为什么要访问它？
- 是否有迹象表明设备已被物理篡改？

如果您长时间与设备失去联系，并且您认为有可能被安装了某些东西，请考虑以下事项：

- 计算机：从头开始重新安装操作系统，并从上次的备份中恢复所有文档，并且要使用防病毒软件扫描所有文档和文件。
- 手机和平板电脑：建议不要再次使用这台失而复得手机或平板电脑了。如果您无法更换设备，但怀疑它可能会受到损害，请采取预防措施，不要使用这部手机或平板电脑进行敏感通信或打开敏感文件。在参加敏感聚会时不要随身携带，不要在讨论敏感话题时随身携带。

[image]

激进社区用户请从这里进入：[image]防篡改准备

以及这里：[image]恶意女仆和查抄

[image]

恶意软件

“恶意软件”可以令其他用户、政府或第三方未经授权接管您的设备，以执行监控，例如记录击键，窃取密码，截屏，录制音频，视频等。目前国家赞助的攻击者正越来越多地将恶意软件作为监视、间谍和破坏的工具。

恶意软件用于获取设备控制权，利用对设备的访问来发送垃圾邮件，窃取银行、电子邮件或社交媒体凭据，关闭网站，并从记者、人权维护者、非政府组织、活动家和博主那里收集重要信息。

[image]

激进社区用户请从这里进入：恶意软件

如果您怀疑设备上存在恶意软件感染，您可以执行以下操作。

首先回答一些简单的问题：

- 您确定这不是帐户劫持或密码泄露？
- 您的妥协指标是什么？

什么是妥协指标？ —— 您可能认为您的设备感染恶意软件的原因有很多; 这些就被称为“妥协指标”。它们可能包括以下内容：

- 您打开了一个您认为可能是恶意的附件或链接；

- 不使用网络摄像头时，您的网络摄像头 LED 会亮起来；

- 即使您更改了密码，您的帐户也多次遭到入侵；

如果出现以下情况，您可能还有理由怀疑您的设备是否感染了恶意软件：

- 您的设备被扣押，然后被退还；

- 有人闯入你的家，可能已经篡改了你的设备；

- 您的一些个人数据已被公开，那些数据只能是来自您的个人计算机；

- 您的团队成为政府、执法部门或具有同等能力的攻击者的目标；

缓解问题

在确认它不是帐户劫持并且有明确的妥协指示后，有两种方法：清洁您的设备或了解攻击类型然后再清理您的设备。找出发生了什么、以及谁伤害你，对你来说不那么重要。但是，了解您的对手，他们的技术能力以及潜在的攻击者（政府实体或其他第三方）是否已知使用了互联网监控技术，可能非常有价值。如果了解攻击者和攻击与您相关，那么在您“清理”计算机之前收集和分析有关潜在恶意软件感染的信息，这点至关重要。否则，建议采用一级分析师的步骤，请继续执行以下部分。

‘清洁’您的设备

如果您选择在不了解恶意软件和攻击的情况下清理设备，请记住以下

几点：

1. 没有非常快速的修复方法。即使在完成以下步骤之后，仍可能存在非常复杂的恶意软件感染。当然，这些步骤足以删除您可能遇到的大多数恶意软件，除非您遭受的是高级攻击。

1. 如果您认为自己是国家级攻击者的目标，并且在清除通过以下步骤检测到的病毒后仍然存在妥协指标，请将其与互联网断开连接，关闭设备，拔下电源插头，如果可能，请取出电池并寻找安全专业人员的帮助。

反病毒

反病毒软件可以成为保护设备免受大部分恶意软件攻击的有效第一反应。但是，这类软件通常被认为对针对性攻击无效，特别是由国家赞助的高级别攻击者。尽管如此，它仍然是针对非针对性攻击但仍然危险的恶意软件的有价值的防御工具。

以下是一个不很详尽的选项列表：

- Microsoft 安全扫描程序（Windows）

- F-Secure

- 卡巴斯基

- ClamXav（Mac OS X）

- 趋势科技 TrendMicro

- ClamAV（Windows 和 Linux）

运行反病毒软件时，请确保它是最新版的。

如果检测到病毒，建议执行以下步骤。

- 第1步：确保您的反病毒软件是最新的；
- 第2步：截取消息的屏幕截图；
- 第3步：继续执行建议的步骤以删除病毒；
- 第4步：按上面“安全通信”部分中的指导原则，将屏幕截图发送给具有安全专业知识的技术人员

[image]

DDoS 缓解

许多独立记者、反叛运动官方网站运营者和博主可能面临的威胁通常是网站瘫痪或被入侵。“拒绝服务”攻击或网站接管是其中最常见的。

上面这一部分已经引导您完成诊断潜在问题的一些基本步骤。如果您的网站受到拒绝服务攻击，建议您采取一些后续步骤。

网站可能出现故障的原因有很多。大多数情况下是由于托管网站的公司的编程错误或技术问题。有时候，法律挑战等其他因素也会导致主机关闭网站。如果您没有托管专业知识就会很麻烦。

因此，在可能的情况下，最好的第一步是联系可以帮助您网站的受信任的人 。

在调查下面的这些常见挑战后，最好联系您的网站管理员和网站托管服务商。

首先回答一些简单的问题：

- 谁建立了你的网站？他们可以提供帮助吗？
- 谁是您的网络托管服务提供商？如果你不知道，可以使用一个工具以帮助查找。
- 您是否拥有此帐户提供商的帐户登录信息？
- 您在哪里购买了域名？在某些情况下是指您的网站托管，但也可能是另一家公司的；
- 您是否拥有域名服务的登录详细信息？如果没有，找到这些是恢复网站的第一步；
- 还有谁知道或可能有权访问这些帐户详细信息？

诊断信息

您的网站关闭的原因可能不同。以下部分解释了每个问题是什么以及如何诊断具体问题。

- 您的网络托管服务器有效但网站不可用吗？

检查 downforeveryoneorjustme.com 您的网站可能已启动但无法看到它。这是一个网络问题，您自己的网络连接可能存在问题或阻止您访问您的网站。这也可能表示您的帐户已被停用：是否看到来自您的网络托管服务提供商的邮件？可能是因为结算、法律、版权或其他原因而被下线。这是一个政策问题。首先，请确保您的结算信息是最新的，并且托管服务或域名没有未结余额。如果该消息是由于法律问题引起的，那么 EFF 提供的资源在关注美国版权法的同时，也是了解更多信息的好地方。

- 您的网站根本没有加载吗？

您的托管公司可能有问题。您能访问托管公司的网站吗？请注意，这不是您自己网站的管理部分，而是托管您网站的公司或组织的管理部分。查看或搜索“状态”博客（例如 status.dreamhost.com）; 还可以在 twitter.com 上搜索其他讨论该主题的用户（搜公司名称）。

- 您是否可以访问与您的网站具有相似内容的其他网站？

尝试访问与您相关的网站。也可以尝试使用 Tor 或 Psiphon 访问您的网站。如果这有帮助，说明您遇到的是阻塞问题 — 就是您的国家和地区出现了网络封锁。

- 您看到了错误信息了吗？

这可能是一个软件问题。您应该反思团队最近可能做出的任何更改，并与您的网站管理员联系。发送屏幕截图给他们。您也可以将错误消息复制到搜索中，以查看它们是否易于修复。

- 您是否从浏览器收到了有关您自己网站上的恶意软件的警告？

这可能是一个污损问题。您需要与您的网络托管服务提供商合作，并查看帐户劫持部分。

- 您的网站是间歇性加载还是异常缓慢加载？

网站可能会被其接收的页面请求的数量和速度所淹没 — 这是一个性能问题。这可能是“好事”，说明您的网站正变得更受欢迎，并且只需要一些改进来响应更多读者 — 检查您的网站分析。许多流行的博客和 CMS 平台（Joomla，WordPress，Drupal 等）都有插件来帮助您在本地缓存您的网站并集成 CDN，这可以显著提高网站性能并恢复能力。

[image]
[image]

S12我盟-总章节

[image] 关键词

[image] 创建时间 2025年1月1日

[image] **Description** 自我照护和互助

“坚强独立”是无依无靠之人报复性自虐的誓言。

[image]

[image]

建设中！敬请期待。

[image]
[image]

直接行动的组织形成-黑群及其他：我盟S12E01

[image] 关键词	
[image] 关联	[image]S12我盟-总章节
[image] 创建时间	2025年1月2日
[image] **Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

亲密、身份认同和策略：我盟 S12E02

[image] 关键词	
[image] 关联	[image]S12我盟-总章节
[image] 创建时间	2025年1月3日
[image] Description	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

工作中遇到问题。你认为管理层不公平。该从哪里入手？ - 我盟S12E03

[image]	关键词	
[image]	关联	[image]S12我盟-总章节
[image]	创建时间	2025年1月4日
[image]	**Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

开始组织-基础知识手册：我盟S12E04

[image] 关键词	[image]S12我盟-总章节
[image] 关联	2025年1月5日
[image] 创建时间	自我照护和互助
[image] **Description**	

[image]

[image]

建设中！敬请期待。

[image]
[image]

“一对一”的艺术：我盟S12E05

[image]	关键词	
[image]	关联	[image]S12我盟-总章节
[image]	创建时间	2025年1月6日
[image]	**Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

每朵玫瑰都有刺-我盟S12E0N

[image] 关键词	
[image] 关联	[image]S12我盟-总章节
[image] 创建时间	2025年1月7日
[image] **Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

启动一个无等级的直接行动小组指南：我盟S12E06

[image] 关键词		
[image] 关联	[image]S12我盟-总章节	
[image] 创建时间	2025年1月7日	
[image] **Description**	自我照护和互助	

[image]

[image]

建设中！敬请期待。

[image]
[image]

如何组织会议：我盟S12E0N+1

[image] 关键词	
[image] 关联	[image]S12我盟-总章节
[image] 创建时间	2025年1月7日
[image] Description	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

S13互助生存-总章节：共生的自由状态

[image]	关键词	
[image]	创建时间	2025年2月28日
[image]	**Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]

如何进行游击分享：互助就是如此简单S13E01

[image] 关键词	
[image] 关联	[image]S13互助生存-总章节：共生的自由状态
[image] 创建时间	2025年3月1日
[image] Description	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]

团结而非施舍：互助生存S13E02

[image] 关键词	
[image] 关联	[image]S13互助生存-总章节：共生的自由状态
[image] 创建时间	2025年3月2日
[image] **Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

构建互助项目：互助生存S13E03

[image] 关键词	
[image] 关联	[image]S13互助生存-总章节：共生的自由状态
[image] 创建时间	2025年3月3日
[image] **Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

香港生存危机中的反叛政治：互助生存S13E04

[image] 关键词	
[image] 关联	[image]S13互助生存-总章节：共生的自由状态
[image] 创建时间	2025年3月4日
[image] **Description**	自我照护和互助

[image]

[image]

建设中！敬请期待。

[image]
[image]

从组织到行动：极简战术手册

[image] 关键词	团队 战略图谱 直接行动 组织 街头
[image] 关联	[image]S13互助生存-总章节：共生的自由状态 ；[image]S12我盟-总章节 ； [image]直接行动分步指南：它是什么、它有什么用、如何获得成功 ；[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年12月1日
[image] **Description**	自我照护和互助

从零开始。任何人都可以。

- Table of Contents
  1、拓展你的网络
  与您所在的社区进行对话
  从简单的对话开始：
  根据具体对象的实际需求来针对性提供帮助：
  建立网络的网络：
  增强和安全：
  2、保护彼此的安全
  始终都要结伴而行：
  为被捕者提供支持：
  建立安全屋和支持网络：
  不要和警察说话：
  不要吹嘘自己的功绩，也不要吹捧其他队友所做的事：
  不要轻易指控渗透：
  3、走上街头
  保持团结：

使用路障：
保持前进：
列队前进：
4、居安思危
衣服
面罩
头盔
手套
雨伞
使用现金
5、扑灭催泪瓦斯榴弹
6、共同准备
关爱彼此：
保卫彼此：
分发：
沟通：
7、如水
填满咱的工具箱：
明智机动：
共同学习：
勇于创新：

[image]

1、拓展你的网络

每场起义都需要大量的“后方”人员和人际网络的支持。

加强前线人员与那些有希望承担支持角色的后方社区之间的联系，至关重要。

[image]

返回：https://iyouport.substack.com/p/3--7bf?utm_source=publication-search

返回：[image]S01E03-T1 周围是谁？可视化人际关系图谱

与您所在的社区进行对话

从最近的身边开始。深化现有的关系（家庭、邻居、朋友等），使其成为支持网络的潜在联系。

从简单的对话开始：

亲自登门拜访。或者去到目标人群最聚集的地方。交流，找出对方可以提供帮助的切实方法。

延伸：https://iyouport.substack.com/p/9-a70

根据具体对象的实际需求来针对性提供帮助：

让您的联系人在他们自己最亲密的人脉圈中重复这个过程。

正确的问题比正确的答案更重要。

建立网络的网络：

寻找各种社会组织中人脉广泛的人，并询问他们在什么情况下会利用自己的影响力来提供支持。

也不要一味的相信承诺，要具体衡量抉择的可能性。

延伸：https://iyouport.substack.com/p/5-

增强和安全：

以安全为前提，制定协议，以高效的方式共享信息、需求和材料。

[image]

返回：[image]信息最小化原则 ；[image]数字技术限制和最佳实践

2、 保护彼此的安全

认真对待安全问题，但要避免过度猜忌。我们可以通过一些简单的措施来保护彼此。

始终都要结伴而行：

不要独自一人到达或离开示威现场。

如果你觉得有人跟踪你，那就先别回家，也不要去同伴家里，去一个无关紧要的地方比如小酒馆或商业街。

直到你确认甩掉了跟踪，再回家。

[image]

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

为被捕者提供支持：

保释、监禁其间的各方面支持、和法庭支持，都是至关重要的。为保释和法律辩护筹款。

[image]

返回：[image]被捕支援

建立安全屋和支持网络：

人们可能需要躲藏起来，寻求物质和情感上的支持。现在就制定计划，尽可能妥善。

[image]

返回：[image]藏匿点或安全屋 ；周密的行动计划

不要和警察说话：

和警察说话不会有任何好处。如果警察来找过你，一定要告诉你的同伴。

[image]

返回：[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

不要吹嘘自己的功绩，也不要吹捧其他队友所做的事：

敏感信息绝对不该公开分享。

杜绝功利心，在安全方面至关重要。

不要轻易指控渗透：

除非你已经掌握了切实证据，否则不要轻易指控渗透者。不要揣测动机。

如果你的直觉显示某人不可信，那就不要跟他们合作。这是你能做的最好的事。

在没有确凿证据的情况下，不要轻易指控。

怀疑和逼供是警察才会干的事。尤其是，很多情况下指控渗透只会掀起群体恐慌，影响行动，令镇压者受益。不如行动结束后再议。

3、走上街头

仅仅谴责统治暴力是没有意义的。统治者根本不在乎。除非能采取实际行动以扰乱这台统治机器。

有时，象征性的目标在战术上最没用 —— 想想看，哪个威胁更大：是在空荡荡的市政厅举行的下班后集会呢，还是在交通高峰期阻塞高速公路的突击性示威活动？

保持团结：

不要让警察分散我们的队伍。

行动中与队友保持紧密联系，不断重新集结，保持恰当的距离，切勿背对着对手 —— 如果被包围的话，采取队友间背靠背阵型，尽可能减少防御盲点。

战术共识应该在行动开始之前确立。行动一旦开始，直接排除违反共识的人即可（那有可能是渗透者）—— 切勿 因个体错误将行动者队伍分成“好的”、“坏的”，那只会为警察提升镇压力度提供理由。

[image]

返回：[image]直接行动的组织形成-黑群及其他：我盟S12E01

使用路障：

将堆砌物拖放到游行队伍后方，以隔离可能的交通和警察的冲击。

[image]

返回：[image]了解防暴弹药，以及如何保护自己 ：示威参与者指南S05E10

返回：[image]从雨伞到激光、气球到电动工具：街头实战指南S05E05 - 战术器具综述

保持前进：

警方可能会试图包围游行队伍，进行“围剿” —— 称之为“水壶”，并大规模逮捕所有人。保持前进，尤其是在十字路口等易受攻击的地形。

在行动前规划路线时要考虑周全。避开桥梁。撤离路线也要准备好。

[image]

返回：[image]地形侦查 ；[image]监视器排查

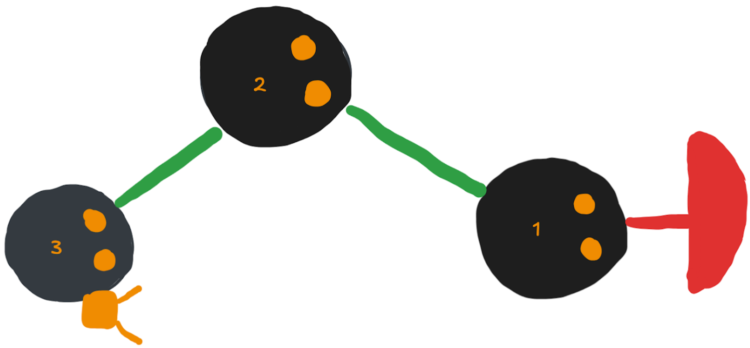
列队前进：

练习与队友们一起“堆叠”前进。保持队伍整体的齐心协力，互相扶着肩膀或背包。

以下是三种堆叠阵型 ——

1. 保持前方掩护，即1号，防止人群受到摄像头监视；同时保持背后的掩护，即3号。首尾要呼应，当危险出现时可以以最快速度传递警告。

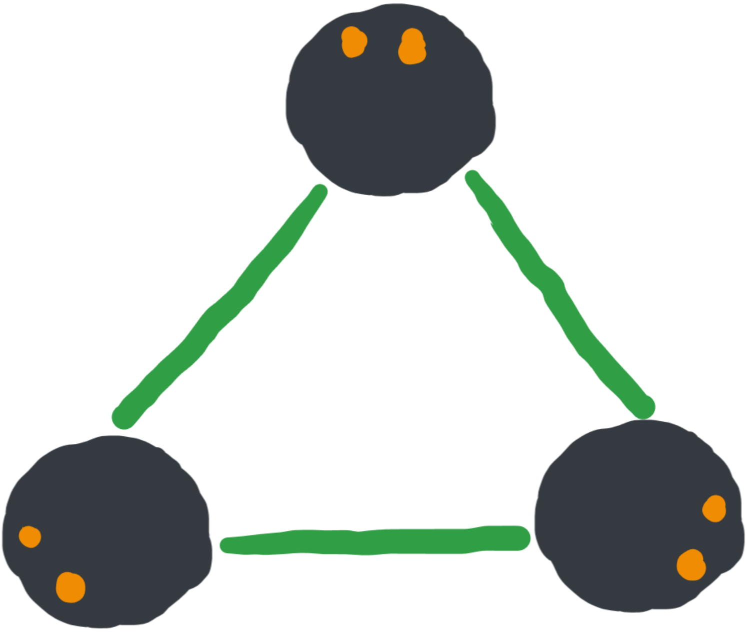
[image]



2、当人群爆发斗殴，混乱加剧时，可以采取这种背靠背的阵型，以及时应对危险。这个阵型也可以让队友们能够清晰地看到现场情况。

如果你们被镇压者包围了，并且觉得肯定会被逮捕的时候，可以彼此挽住胳膊，把阵型拉紧，保持整体的“沉重”，可减轻其中单个人员被警察拖走的可能性。

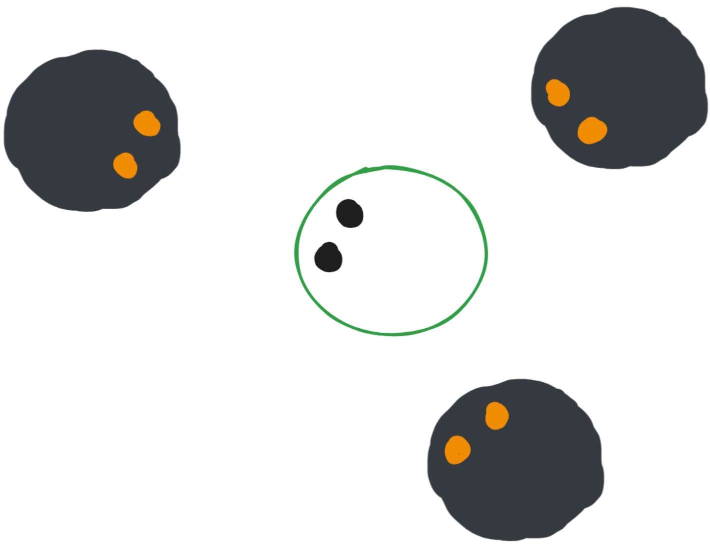
[image]



3、当将不良分子从人群中驱逐出去，或者与对手主动交战时，最好采取三点包围策略，以便更好地控制交战。假设图中白色的是对手。

后方人员应准备好抓住对手，而其他两人则负责威慑或武力。

[image]



4、居安思危

只要做好准备并配备合适的装备，我们就能防御警察的防暴弹药。

衣服

穿不显眼的衣服。衣服上不要有任何标识、不要有鲜艳的色彩。因为警方将事后审查监控录像以确认嫌疑人身份，如果您穿得回头率太高或者太容易被描述，会对您不利。

遮盖任何可用来识别您的纹身、穿孔、疤痕、发型/发色等。

[image]

返回：[image]匿名着装

返回：[image]在街上保持安全：街头实战指南 S05E12

面罩

全脸呼吸器或半脸呼吸器与护目镜搭配使用，可防止化学武器和警用弹药对眼睛的伤害。

务必遮住脸部，以防被认出。

[image]

返回 - 选面罩的方法：[image]抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

头盔

戴上不显眼的头盔（如棒球帽或自行车头盔）可以一定程度上防止橡皮子弹、榴弹和警棍造成的头部创伤。

[image]

返回 - 选头盔的方法：[image]头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

手套

手套可以确保不留下指纹。

并且，如果您需要丢弃警用催泪弹，耐热的消防手套或皮手套可以保护您的双手。

[image]

返回：[image]在街上保持安全：街头实战指南 S05E12

雨伞

雨伞可以挡住警察的弹药、阻挡胡椒喷雾，还能躲避警察和媒体的摄像机。

使用现金

尤其是回家的交通支付，一定要使用现金。任何在线支付都会导致追踪。

包括所有与抗议活动有关的装备，也都要用现金购买。

[image]

返回：[image]匿名购买 ；[image]匿名着装

最好能携带一套普通日常的衣服，以便在活动结束后立即换上。

尽可能不要带手机！至少不建议携带私人手机。

[image]

返回：[image]匿名手机

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

5、扑灭催泪瓦斯榴弹

戴上防热手套和防毒面具，将催泪弹浸入宽口水壶中，水壶中每升水放3汤匙小苏打、洗洁精和/或植物油。用一只手盖住瓶口，以防止气体溢出，然后摇晃水壶。

切勿密封装有催泪弹的瓶子，以免发生爆炸。

您还可以使用防热手套将催泪弹从人群中扔出去，或用棍子将其打飞。

吹叶机可以迅速驱散催泪瓦斯，保持空气清新和可呼吸。

[image]

返回：[image]了解防暴弹药，以及如何保护自己 ：示威参与者指南 S05E10

6、共同准备

现在是获取物质资源、建设基础设施和发展支持系统的时候了。从疫情到动荡，再到自然灾害，互助始终都是是集体力量的基础。

关爱彼此：

规划从身心健康、住房、到种植粮食等各方面的技能和物资。汇集资源，帮助有需要的人。

保卫彼此：

社区自卫的范围从缓和冲突到实际干预。

建设坚韧的社区，让警察和所有国家机器都不受欢迎。

推动反抗蔓延，声援那些已经遭受压迫的人们。

[image]

返回：[image]开始组织-基础知识手册：我盟S12E04

分发：

以分散、协调的方式分享技能和物资。制定物流策略，将人员和物资从一个地方运送到另一个地方。多元化角色，打造更强大的运动。

通过培训和协助，尽力让大家有能力承担不同程度的风险。

沟通：

做好数字安全措施。使用端对端加密和一次性手机。

如果数字网络出现故障或变得不安全，请制定其他通信方案，例如双向无线电或人力信使。

[image]

返回：[image]数字技术限制和最佳实践

7、如水

自然之道如水之道。无关利益，无关功利，不自私，无奢想，涤除玄览。大成若缺，大盈若冲。

尽管我们没有现代化的武器装备，但我们有足够多的同道、丰富的智慧、适应性和机动性。

[image] FBI文件，将BeWater策略列为“非法”

填满咱的工具箱：

不要排除那些对你来说可能陌生或不舒服的战术。

辩论是健康的，但所谓的“暴力”与“非暴力”的对立只是幻象。

明智机动：

根据地形进行调整。真诚地处理你认为是错误的行动。

根据具体目标调整战术和阵型。

事先讨论利弊。事后进行汇报。

[image]

返回：[image]充分的准备和应急反应同样重要：整体安全S01E07 - 计划是 “活的”

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

共同学习：

将每一次行动都视为下一次行动的训练。反思哪些有效，哪些无效。与他人分享你的见解。

勇于创新：

当一种战术达到极限时，就要去尝试一些新的东西。

相比那些等级森严的镇压部队，我们最大的优势就在于能够快速发展，并采取不对称的行动。

延伸：https://iyouport.substack.com/p/40

起义只有在保持复杂性、多样性和感染力的情况下才能成功。

只要行动开始，所有加入进来反抗暴政的人 都是战友 —— 无论是通过静坐、通过游行还是直接对抗。不要谴责与你不同的战术。

拥抱所有那些与我们并肩作战的人 ，我们就能保护每个人免受最终降临到我们所有人身上的压迫。

为了维持一场能够克服分歧、改变历史进程的运动，我们都必须承担一定的风险。

[image]
🎀

人际安全&关系结构革命-RelationshipsRevolution

“你是谁？” - 这个问题的答案往往只是由一大堆身份拼凑而成。这就是导致我们之间难以切实连接的根本性错误。 导致人被工具性评估。导致关系以结果为导向，并因此充斥着始终无法满足的愤懑。 无政府主义革命正是在致力于构建一种关系结构，在这种关系中，没有任何人能够系统性地支配或压迫他人， 因为权力分配均匀，合作比残酷的竞争更有激励作用。 它就是威权主义的对立面。

[image]
[image]

是什么导致队友间不分享知识？

[image] 关键词	协作 团队 沟通 竞争 等级制度 组织
[image] 关联	[image]S11关系结构革命-总章节；🚶不是“个人问题”
[image] 创建时间	2020年6月4日
[image] Description	关系结构革命

人们会下意识自私，但这并非无法解决。

- Table of Contents
1、是什么促使人们分享或隐藏知识？
2、什么样的工作会促进知识共享或导致隐藏？
3、当人们依赖你时会发生什么？

BACK 🚶不是“个人问题”

[image]

也许您早已有这样的体会：在互联网上，只有那些口水的和浅薄的（一次性的、没有保留价值的）内容会被更多人分享，但是，实用性的知识被分享程度会极低。

曾经很多人对这种现象做出过自己的解读，从虚拟空间的娱乐化到行动力差、从算法操纵到回音壁气泡 …… 也许，各种原因都有，但是，一些更明显的原因被忽略了。

我们先抛开互联网媒介。如果你曾经在一个团队中与其他人协同工作，不论是公司还是基层组织，也许你已经有这样的体验，即：某些

工作只能某个人来完成，而此人往往不会倾向于教会更多其他人关于如何完成这件事的技术和经验，即便你很想学，也经常会遭到委婉的拒绝。

这是为什么呢？

这个问题的答案与开头第一个问题的答案是一致的：大多数人不会倾向于分享高质量的知识 —— 也就是那些你无法从教科书中获得的东西，它必须来自大量的实践。于是它往往是私人的。

这是件麻烦事。不论您是公司管理人员，还是公民社会组织者，您都会期待您的下属和队友彼此分享知识；因为，毕竟，这样可以为个人、团队和组织带来更大的创造力、更多的创新和更好的性能。

然而，尽管组织者试图鼓励知识共享，但许多成员还是隐瞒了自己所知道的东西 —— 这不是罕见的，这种现象被称为知识囤积或知识隐藏。

在需要分享知识的时候，人们会下意识装傻，假装不知道某些东西，或者承诺分享但从来不这样做，或者直接告诉别人不可能共享。

《组织行为学杂志》上的一篇研究发现，工作的设计方式会影响成员是否向同事共享知识或向队友隐藏知识。

具体来说，认知上更为复杂的工作（人们需要处理大量信息并解决复杂的问题）这种情况下倾向于促进更多的知识共享，而提供更多自治的工作也有可能促进知识共享。

[image]

而在竞争环境下，最主要的就是抑制成员之间的知识共享。

现在你知道的了，由于互联网鼓励的是竞争，人们彼此间更多是为了争夺更大的自身影响力；这种情况会明显压制知识的流动，并鼓励那

些肤浅的观点占据大部分流量 —— 人们倾向于转发后者是由于它们代表 “我的立场”，积累 “我的” 声誉。

[image]

延伸：https://pao-pao.net/article/837

这项研究收集了来自澳大利亚各个组织的394名知识工作者和中国一家出版公司的195名知识工作者的数据。

研究人员对参与者进行了调查，以了解他们在工作上的认知需求、他们的自主权以及同事之间在工作上的依赖程度。还询问了他们与他人分享知识的动机。

几个月后，研究人员要求参与者报告与同事共享知识的频率、以及他们认为该知识有用的程度。

分析得出了三个关键发现：

- 首先，人们出于不同原因共享和隐藏知识；
- 其次，如上所述，当人们从事对认知有要求的工作并拥有很多自主权时，他们会更愿意分享知识；
- 第三，如果他们认为同事过于依赖他们，就更有可能隐藏知识。

下面逐一介绍一下。

1、是什么促使人们分享或隐藏知识？

在分析有关动机的数据时，研究人员将其参与者的回答归类为 “自主动机”（这意味着做某事是因为它有意义或令人愉快）、或“受控动

机”（这意味着要做某事是为了获得奖励或避免惩罚）。

研究结果表明，当成员具有自主动机时，知识共享就更有可能 —— 例如，他们同意 “与队友分享我所知道的事可能很重要”、或 “谈论我所知道的事很有趣” 这样的想法。

相反，当人们的动力是由外部压力驱动时（比如 “我不想受到批评” 或 “不这样做的话我可能会被排斥”），人们反而更有可能隐藏自己的知识。

这意味着，迫使人们分享知识而不是让他们看到知识分享本身的价值，就不会有好的结果。

如果你的队友不了解共享知识以达到组织目标的重要性，那么他们共享该知识的可能性就很小。

并且，如果你的队友被迫分享自己的知识（比如你把这条写入组织规范了，并添加了隐藏知识的惩罚方式），那么就很可能适得其反。

如上所述，如果人们害怕失去竞争优势，他们就更不愿意透露信息了。

但要知道，这其中可能有社会文化方面的作用。在这项研究的中国样本中，上述 “受控动机” 与知识共享的频率增加有关，但与共享知识的更大效用却没有关系 —— 简单说，在中国的案例中，人们更可能会在惩罚压力下共享知识，而非对共享本身的价值的认同。

所以，在组织运作中，作为领导者您应该考虑文化因素。

2、什么样的工作会促进知识共享或导致隐藏？

对认知的要求很高的工作可能会更加有趣和刺激，并且也更加困难和充满挑战，于是您会希望队友既喜欢共享信息、又能看到共享的更大

利好。

同样，由于在工作中拥有更大的自主权会导致发现它更有意义，所以您会希望看到同样的分享倾向。

这项研究的结果支持了这些想法。

当人们的工作涉及较高的认知要求和自主权时，他们会更频繁地共享有用的知识。澳大利亚和中国的知识工作者在此都一样。

3、当人们依赖你时会发生什么？

知识工作在很大程度上取决于组织中各个成员所拥有的有形和无形知识（例如，数据和专业技术），这会在员工之间造成相互依赖。

因此，一个人可能需要来自各方的信息才能有效完成其工作。

如果您依靠同事的知识来完成工作，那么可能会通过与他人共享知识来使自己更有可能做出回报。这是一种凝聚力。

除了询问受访者有关他们如何与同事分享和隐藏知识外，研究还询问他们是否依靠同事来完成工作。研究人员希望看到如果受访者认为他们的同事依赖于他们，他们将更愿意分享知识，而不太可能隐藏它。

但令人惊讶的是，结果完全相反。

当人们意识到他人依赖自己时，他们会感到压力（动机的受控类型），从而更加倾向于隐藏知识。

这也许是队友的依赖性占据了他们太多时间，时间是一直稀缺的资源。这种情况下人们甚至会撒谎，假装自己没什么可以提供的。

当然，与所有研究一样，这项研究也有局限性。

首先，没有考虑参与者共享知识的性质。有人可能会说，如果队友喜欢分享自己的知识（自主动机），这可能会导致他们分享更多的隐性知识（更难以记录和转让的内在专有技术），而不是显性知识（清晰的教科书信息）。

其次，研究数据仅限于员工的自我报告。如果将来的研究可以收集其他数据，例如队友之间的共享数据、有用性、拒绝次数以及原因，结果会更好。

有效的知识共享对于所有组织来说都是必不可少的，但是许多组织都在努力劝导成员这样去做，却往往事与愿违。

[image]

这项的结果表明，作为组织者，如果您想要鼓励队友之间更多的共享，那就首先需要设计您的工作本身，以便人们想要讨论他们所知道的东西。

不论是社区、团队、组织或者公司，管理都是一项复杂的工作；您可以在实践中获得经验，虽然这会导致太多的试错，当然也可以通过科学研究的结论找到灵感。希望这篇文章对你有用。

不要错过我们推荐的资料👇，在这里下载这份手册：https://t.me/iyouport/6779

[image] 下载手册：

[image]
[image]

建立国际团结：全球斗争中的人际关系

[image] 关键词	关系 协作 联合
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2021年11月30日
[image] **Description**	关系结构革命

通信是激进斗争的倍增器。它使我们能够联合起来，给当权者制造更多的压力，而这也是当我们作为孤立的个体时无法做到的。

- Table of Contents

从本地、到大陆、到国际网络
1、您自己的国家/地区
2. 大陆/群岛组织
3. 国际团结和行动
交流方法
1. 数字化
2. 电话/无线电
3. 亲临现场
基本技能
1、语言
2. 文化知识
3. 对界限的相互理解
最后：只需伸出手

[image]

在去年底的对话中，我们特别强调了国际联盟的重要性。因为我们所有人对抗的都不仅仅是一个政权和几个政客，而是一个系统，这个系统在地球上每一个角落发挥作用，反抗者的联合正是该系统旨在重点防止的东西之一，因为这对它是致命的。

换句话说，这不仅仅意味着没有任何问题属于纯粹的“本土问题”，并且意味着，“我们”的结盟就是对战“他们”的武器。

在过去的30年里，这个世界已经进入了一个新的通信时代，无政府主义者祖先们曾经只能梦想我们有这样的能力与世界各地志同道合的无政府主义者迅速沟通。但重要的是要记住，有效的、具有历史意义的国际团结和沟通网络早已存在，就像无政府主义组织本身那样古老。当芝加哥干草场的烈士们牺牲时，全世界的劳动人民通过通信网络传播消息，发出了愤怒的声音；当墨西哥活动家里卡多·弗洛雷斯·马贡（Ricardo Flores Magon）在尤马地区监狱的牢房里饱受折磨时，是像琼斯夫人和艾玛·戈德曼这样的人利用他们的网络大声疾呼，倡导释放他。

[image]

通信是激进斗争的倍增器。它使我们能够联合起来，给当权者制造更多的压力，而这也是当我们作为孤立的个体时无法做到的。

尽管技术在不断进步，但激进主义者的通讯能力却没有跟上步伐。当然，许多无政府主义者一直在通过公报、新闻报道或社交媒体帖子了解其他斗争，但在这些偶然的互动和有意义的关系建设之间存在着深刻的裂痕，而这些关系是有弹性的、有效的和有意义的斗争所必需的。

本文希望概述一些基本的组织网络、沟通方法和必要的技能，以便在对抗殖民主义、资本主义和反统治的斗争中与无政府主义同伴建立更深的关系。请记住，这仅仅是单方面的建议；建立关系是一件非常复杂的事，而且往往是个人的事（如果做得好的话）。您要想真正知道该如何做，唯一的办法就是去尝试。

[image] Bangkok, Thailand

从本地、到大陆、到国际网络

1、您自己的国家/地区

在您自己的地区的交流应该是最常规的交流形式。这涉及到一个共同商定的区域的人们定期聚集在一起，分享即将发生的事，讨论区域问题，在适当的时候制定联合努力的战略，以及作为人的基本社交模式来建立联系。

这些可以遵循严格的安全规则，只有成员选定的代表在需要时组成分组，以讨论敏感项目。我们已经发布过一些指南，关于讨论和组织敏感谈话的方法，以尽量减少泄密或告密者的损害风险。

[image]

激进社区用户请从这里进入：[image]信息最小化原则

更广泛的社交活动中应尽量减少要讨论的话题的敏感性，并应致力于通过共同的活动建立关系（有些人可能想要一个区域性的在线加密群组，有些人可能想要组织实地考察，有些人可能想要去酒吧聚聚，等等，只需要时刻基于您自己的威胁模型）。

2. 大陆/群岛组织

大陆和群岛的组织实际上是在区域/岛屿的个体、集体、同行群体和组织的网络之间进行的，大陆/群岛组织的作用是促进这些区域网络间的沟通，使其进入更广泛的大陆/群岛范围。比如从北京市的美团快递小哥开始，到全国美团快递小哥，到全国零工工人群体、到东南亚零工工人组织。（您可以在这里看到相关故事 https://iyouport.substack.com/p/eb1?utm_source=publication-search ）

各地区可以从整个地区选择一个代表团，或从每个组织选择一个代表团，参与这个大陆/群岛通信网络。这被用来呼吁物质援助（特别是

当某个地区正在经历动荡或灾难时）、寻求咨询、寻求增援、或宣布集体利益的新的行动主义项目。

大陆网络的作用还在于确保许多不同的地区、文化和政治局势有一个快速有效的手段来联系大陆上的每一个其他团体，而不依靠口口相传的低效、没有算法的集中化操纵、也不需要被企业媒体筛查的新闻发布。

由于公路、铁路和陆地边界的连接，大陆环境中的实际聚会和物质援助的转移自然会更容易。群岛地区的聚会和物资援助的转移可能更加困难，因为要提供负担得起的远洋或航空运输，躲避国家海军的巡逻，港口费用，海关等等，都使这些努力难度更大、时间更加紧张。

最重要的任务之一是建立强大的通信基础设施和强大的联系人网络或关系。这些人际关系可以得到发展和培养，同时可以开始想办法把古老的重要远洋网络重拾起来。

3. 国际团结和行动

国际网络对于确保我们的政治不至于对其他大陆巨大的政治发展视而不见，确实至关重要。比如，您可以从整个殖民世界的原住民反抗那里学到很多东西。

反抗者经常被本地的政治思想视野和本土历史上的斗争经验 限制了创新能力 ，这是一种严重的损失。人们忘了遥远的地方也有同样一群人遭受的同样压迫的人，他们一直在挣扎、学习、思考、创造和战斗。如果不与他们联系起来，就等于让我们所有人一次又一次地犯同样的错误。

您可以通过向那些经历过、做过的人学习，以绕过绊脚石，这一点怎么强调都不为过。国际网络对于确保全球北方工业化地区的反抗者与几乎没有货币/物质资源而陷入困境的反抗者分享资源也非常重要。我们必须找到方法，确保我们为最艰难的斗争提供资金和物资。只有当我们与全球各地的同道建立起弹性关系时，才能做到这一点。

[image]

交流方法

1. 数字化

社交媒体、电子邮件和网站都可以成为很好的基本联系方式。通常情况下，您会发现任何一个地区都有至少一两个人的数字存在，而且是用一种主要的语言发布内容的（广泛使用的共同交流的语言）。找到一个人的博客，一篇有他们联系邮箱的文章，或者一个发布无政府主义自治主义或反殖民主义内容的社交媒体账户，就可能找到一个接触更大关系网络的机会。他们自己可能都还不知道在自己的地区还有任何其他人也是无政府主义者，但也有可能他们知道。与哪怕是一个人建立关系，都可以帮助您的组织更好地了解该地区的政治局势和在那里组织起来的人们的需求。

从另一方面讲，作为个人和亲密团队那样的小群体，只要您愿意公开表达自己的价值观和描述您想要的世界，您就有可能吸引到志同道合的其他人，进而加入更大规模的组织。

当然，这需要详细地观察和交流，才能确定是否真的是同道。顶着一个logo头像或者喊几句口号，任何人都能做到，那没什么意义；识别和结盟同道的唯一有效方法是，看到彼此正在为同一个大的战略目标而努力。

2. 电话/无线电

使用电话通常是一个备份选项，有时比数字通信更有挑战性，至少需要把对方的语言说得足够好，以便交流需要讨论的话题。此外，在一些地方，电话/业余无线电可能是一个很大的安全风险，所以必须要注意。

顺便说，目前您仍然可以使用寻呼机，它比智能手机更安全。网上有

相关教程（即便您没有树莓派也没关系）。

3. 亲临现场

组织旅行以建立人际关系可能是非常有效的，可以建立持久的联系。每一个有效的革命运动都使用过这些类型的旅行，从美国的游击队访问墨西哥的马贡主义者，到萨帕塔人最近在世界各地的信使航行，等等。

如果可能的话，请确保这些类型的旅行计划是相互的。这可以确保关系的建立是真正在一个平等的环境中进行的，而不是复制欧洲传教士的救世主身份，那会很令人讨厌。

[image]

基本技能

1、语言

您现在就可以开始发展的主要技能是语言。如果您的小组里有十几位队友，您就已经有足够的人手去学习多种语言。单语主义是一个民族主义项目，多语主义是一个国际主义目标。移民会告诉您，了解三到五种语言的基本对话水平是很常见的。相信您也可以发展这种技能。

这是一个绝对的事实，发展这种技能是发展有意义的团结的一个基本努力。您在国外的同道用您的母语和您说话，而您却不能回报这种努力，用他们的母语说话，这可以接受吗？如果您把整个翻译工作的负担放在那些不仅讲您的语言，而且还讲您希望与之建立团结的人的语言的同道身上，这可以接受吗？毫无疑问，学习一种新的语言是艰苦的工作，但这是您的国际同道们已经在做的工作。

在一个朋友群体中，语言重叠对国际网络和相互学习有很大好处。它确保了语言的冗余，同时也涵盖了足够的语言基础，以建立有意义的

国际网络。

文本的翻译对于分享革命思想也是一项极其重要的任务。译入和译出一种语言可以确保知识上的交叉授粉，使我们大家都不至于落伍或重复工作。即使是翻译得不那么好的文本，也比没有翻译更好。让一群人从事翻译工作也能极大地提高翻译的质量。一些在线翻译工具可以用来翻译大量的文本，更加省时，由志愿者逐一阅读并在翻译过程中进行更正。这样可以节省时间，提高将材料翻译成多国语言的工作效率，使信息共享更加及时。

[image] https://t.me/iyouport/8596

2. 文化知识

文化知识是建立关系的一个重要部分。这并不意味着带着先入为主的文化期望进入国际沟通，但它确实意味着您要善于观察，在假设之前先询问，并适应对话双方的文化需求。

在政治上，不同国家的人们可能还没有处于相同的发展阶段，或者彼此可能不同意所有相同的政治目标，但没有关系，请确保您尊重其他民族的自决权意味着您不会对其他民族的斗争或组织的标准指手画脚。如果某件事情很恶劣，可以说出来。清楚地说明您为什么不同意某些事。如果这是您可以解决的问题，那很好，去试试看；如果不是，就没有必要与那个特定的个人或团体进一步沟通。

3. 对界限的相互理解

如同所有关系中都有界限，在联盟中也是如此，应该从一开始就进行沟通。确保双方都知道并同意哪些话题和战术会被讨论，哪些不会。确保双方都同意互利的安全文化。确保双方都明白将使用什么形式的沟通渠道和语言。

您应该有适合自己的安全文化，这取决于您的具体威胁模型
BACK [image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
。

最后：只需伸出手

还记得吗，您在生活中所拥有的一切，都是从伸出手开始的。在您学会游泳之前您会尝试把胳膊放在水中滑动，您的手伸出来抓住您要攀登的绳子，在迎接新面孔时举起的手 …… 您已经通过伸出手迈出了很多个第一步。通信和联盟也不例外。建立联系本身就是一种革命性的信仰和团结的行为。上好您的第一堂语言课；给您尊敬的、不在您的政治地理范围内的同道发送一个私信；报名参加语言交流活动；去参加一个地区性的聚会；阅读一个不是用您的母语发表的行动主义的新闻博客；开始抽出时间，在真正的革命团结中构建更有意义的联系。

您能做的事有很多，非常多，您可以立即开始。图景已经清晰，现在我们缺少的只是起步。○

[image]
[image]

S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会

[image] 关键词	关系 团队 性关系 性暴力 米兔 革命
[image] 关联	[image]S12我盟-总章节；[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月1日
[image] **Description**	关系结构革命

[image]

警察是我们的对手。从来且永远都不可能是“帮手”。

出了问题时我们绝不会报警解决。这是我们与改良派的主要区别之一。

自治就是我们亲手打理我们自己和彼此间的一切，我们自己做决定，

我们为自己和彼此的安全与福祉负责。

由此团结一致，对抗所有侵害我们的势力。

[image] [image]

[image]

开放不是“随便”，性解放不是滥交。解放者的宽宏大量不是被用来占

便宜的。请让与你接触的每个人了解并理解这件事。

我们致力于变革的是结构和生态 - 是那个制造悲剧的惯习和土壤，这绝非易事。原谅暂时的混乱和不堪不意味着屈服。我们将始终努力寻求更好的解决方案。

在此，我们的目标是：解决我们彼此间的问题，并同时避免留下导致敌人趁虚而入的破绽，且解决方案理所当然地应符合我们共同信仰的解放斗争政治理念 —— 正基于这份理念，我们呼唤彼此为同道。

风靡全球的米兔战术并不完全符合我们的目标。至少，众所周知且显而易见的，它并没能显著阻止性暴力的发生率，但却同时，甚至在一定程度上已经被渗透者所利用，让国家暴力机器占了便宜。

S09系列希望帮助那些对传统做法失望的人们、和受到困扰并意识到事情不该如此的圈内同道们，探索一些我们可能尚未深入尝试的新方法，以便能有更多智者洞察到现有战术的提升空间。

列表

[image] 是否有比米兔更好的解决方案？如何？：超越米兔S09E01

[image] 恢复团结：超越米兔S09E02

[image] 直击性骚扰和性侵犯的根本：超越米兔S09E03

[image] 搬弄权力 - 性癖好与虐待的本质区别 ：超越米兔S09E04

[image] 社群集体如何帮助私人亲密关系中出现的问题？：超越米兔S09E05

……

不断成长中。

[image]
[image]

是否有比米兔更好的解决方案？如何？：超越米兔S09E01

[image] 关键词	个人 关系 团队 女权主义 性暴力 治愈 米兔 纠纷 组织 自治 问责
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月2日
[image] **Description**	关系结构革命

打破僵局 —— 真正解决激进派反贼圈子中的性侵和虐待问题。

- Table of Contents

  引言
  入门：起源与宗旨
  性别框架
  修复式和转变性正义
  我们所处的境地
  无政府主义社区问责制：近期历史与现状
  社区问责流程的十大陷阱
  1) 缺乏明确的终结标准，也无从界定成功或失败。
  2）成功的标准往往脱离实际。
  3）我们缺乏实现诸多诉求的集体能力。
  4）我们缺乏咨询、调解和冲突解决方面的技能。
  5）这类事务令人沮丧且高度耗费心力。
  6）问责流程吞噬了过多的时间和精力。
  7) 亚文化纽带薄弱到人们轻易就能脱离。
  8）集体规范助长并纵容不负责任的行为。
  9）对抗性司法体系的残余影响正侵蚀着我们对社区问责模式的应用。

10）性侵问责的措辞与方法被应用于并非其初衷的情境。
新方向与后续问题
方向一：幸存者主导的自发维权
方向二：通过性别组织实现预防
方向三：不只是问责，更是解决冲突
方向四：同心圆式的亲密圈
结语
附录
参考文献
书
小册子
其他资源

[image]

首先，推荐一部纪录片，讲述了温尼伯湖畔的奥吉布韦族小社区 Hollow Water 是如何应对他们中间发生的性虐待泛滥问题的。

施暴者通常否认、痛苦蔓延，当事人频发成瘾甚至自杀事件。马尼托巴省的司法系统根本无法结束虐待的循环，因此 Hollow Water 社区决定自己处理此事。

施害人被带回家，在社区治愈和量刑圈中接受正义的审判。这种独特的正义模式基于传统做法，让家庭团聚，同时治愈受害者和施害人。

这部影片是对一个社区治愈和创造变革能力的有力赞颂。

https://www.nfb.ca/film/hollow_water/

[image]

性侵犯与性虐待问题持续困扰着一些激进派圈子和活动空间。为此，前线的同志们制定了在国家体制之外相互问责的机制。

但为何这些机制似乎始终难以完善？

本文将考察这些社区问责机制诞生的背景，剖析实践过程中遭遇的困境。

[image]

要突破我们的圈子内部性暴力问题的僵局，就必须重新审视"社群"这一概念本身，将抗争引向新的方向。

[image]

引言

> “我不再相信责任制了……我对现有模式的愤怒与绝望，与我过去投入的精力是成正比的。问责制于我而言，如同苦涩的前任恋人 …… 过去十年我竭力维系这段关系，但结果呢？”—— 安古斯蒂娅·塞莱斯特《安全不过是幻觉：对问责制的反思》

入门：起源与宗旨

性侵犯与性虐待导致我们四分五裂。它们瓦解了社群纽带，摧毁了个人生活，破坏了我们的变革项目与组织建设，暴露了我们这些革命者的理想与现实实践之间的恶劣矛盾，并维持着恐惧与压迫的氛围 —— 女性尤为深受其害。

性侵犯具有政治属性；它是父权制的产物，而非仅仅是个体（通常是男性）对他人（多为女性）造成的伤害。性侵犯与虐待、伴侣暴力、儿童虐待及性骚扰，是男性对女性实施肉体支配的主要手段。性暴力助长着父权制、异性恋霸权、跨性别压迫、年龄歧视与青年压迫、种族主义殖民主义及种族灭绝。因此，反对性侵犯与虐待的斗争，是革命性变革的基石。

近年来，问责程序模式已成为激进派社群处理性侵与虐待的核心工具。本文旨在剖析该模式，以期引发关于激进派圈内应对性侵行为的

诚实的自我批判性讨论，并探索未来发展方向。

本文并非旨在作为社区问责流程的入门指南；它假定读者已具备相关知识，了解这些流程的运作机制（或失效原因）。本文特别借鉴了北美无政府主义、朋克运动及激进行动亚文化，并假定读者理解其背景和术语。如果您对此不熟悉，建议先阅读文末列出的部分参考文献。如果您身为激进派反抗者，且曾在所属圈层中参与过以"问责"之名应对暴力侵害和虐待行为的实践，本文正是为您而写。

性别框架

性别概念复杂多变：某些被他人视为“男性”或“女性”的人士自己并不认同这种性别标签，还有人完全不认同任何性别分类。本文提及"男性"或"女性"时，特指那些认同自身性别身份的人士，无论其为顺性别者还是跨性别者。

在整篇论述中，无论是性侵幸存者还是施暴者，均采用中性代词"他们"进行泛指。性侵与虐待行为可能跨越性别界限发生在任何人身上：顺性别女性、跨性别男性与女性、性别酷儿群体都可能实施侵害，顺性别男性也同样常成为受害者。但这不应掩盖一个事实 —— 绝大多数施暴者仍是顺性别男性，而受害者主要为女性。

[image]

性侵犯与虐待既非特定性别专属（换言它不会发生于特定性别群体中），亦非性别中立（即施暴者与受害者自身的性别与事件本质无关）。我们必须理解性别化的侵犯模式是父权统治的体现，同时避免忽视那些超出此框架的经历。

修复式和转变性正义

谈及问责机制时，我们指的是应对伤害（此处特指性侵犯与性虐待）的集体行动。这类行动不以惩罚或法律意义上的"正义"为重心，而是致力于保障人身安全，并挑战滋生虐待行为的深层社会模式与权力结

构。

即实践意义上的，对事不对人。

从最宽泛的意义上讲，这可能仅指几位朋友为受伤害者发声：询问其需求，并尝试与施害者及共同圈子协商，以满足这些需求。某些程序涉及由团体在个人与指责者之间进行调解，或由不同团体分头支持当事人并促进双方之间的沟通。这些程序通常要求被指责者满足特定条件或"诉求"，以此重建安全感与信任，防止伤害重演，并通过后续机制确保诉求落实。

所有这些方法都旨在绕开国家机器，直接解决既有的伤害问题。

社群问责制对无政府主义者极具吸引力，在于它是对刑事“司法”系统的对抗性框架的一种关键替代方案。后者假定冲突双方利益对立：国家自诩为“受害方”并充当调解人；所谓"正义"实为判定谁正确、谁受惩罚 —— 惩罚由国家决定，通常与实际伤害、尤其是造成伤害的根源问题无关。

相比之下，修复式正义关注受害者与施害者的需求，而非满足抽象法律原则或实施惩罚。受害者在解决纠纷中发挥积极作用，施害者则被鼓励为自身行为承担责任，并修复造成的伤害。

[image]

这种正义观认为"犯罪"与不当行为是对个人或社群整体的侵害，而非对国家的冒犯。

当前许多修复式正义的实践模式源自毛利人和北美原住民社区。

在此框架基础上，转变性正义模式将修复式正义的焦点 —— 即纠正错误和缓解伤害而非强化国家权力 —— 与对系统性压迫的批判相结合。据以该模式为基础开展终止儿童性虐待工作的组织"第五代"所言，转变性正义的目标包括：

- 为幸存者提供安全、疗愈与自主权
- 让施害者承担责任并实现转变
- 社区行动、疗愈与问责
- 致力于彻底改变滋生暴力的社会根源 —— 剥削压迫的体系、支配性结构及国家暴力

无政府主义实践中的社群问责机制，其理论根基正是这些核心原则，同时融合了DIY伦理与直接行动的实践导向。

[image]

我们所处的境地

无政府主义社区问责制：近期历史与现状

这套应对性侵和虐待的实践体系是如何形成的？

在1990年代至2000年代初，女性及其他幸存者通过多种方式应对侵害行为，包括：制作揭露施暴者的独立刊物并在演出场合分发，在幸存者群体内部分享经历，向其他社群警示惯犯行踪，甚至采取肢体对抗手段。俄勒冈州波特兰地区的 Hysteria Collective 是早期系统性应对性侵的尝试之一，他们制作并分发宣传资料，挑战朋克圈中施虐男性的存在，并组织了专题会议。其他城镇则涌现出以自卫和集体对抗为目的的女子帮派。

然而此类行动往往 孤立无援 ，无政府主义者中（尤其是男性中）仍盛行强奸神话， 试图发声的幸存者常遭忽视、排斥，被指责“转移重要议题的注意力”，甚至被归咎为制造分裂的"反情报计划"式行为。

作为回应，无政府主义女性及其他人士致力于推动无政府主义圈层严肃对待性侵与虐待问题，倡导同意文化。这些理念主要通过杂志小册子传播，尤其是辛迪·克拉布的《多丽丝》和《支持》杂志；同时，激进派会议上开始出现探讨幸存者支持、“同意”的原则、及积极性观念的研讨会。在某些激进派圈层中，男性团体开始组织起来反对性暴力，例如2002年在明尼阿波利斯成立的"处理我们的烂摊子"（DWOS）集体。2004年费城 Pointless 音乐节成为重要转折点：主办方公开宣布三名女性在活动中遭强奸，并成立集体组织支持幸存者及处理施暴者。这些集体后来发展为"费城愤怒者"与"费城挺身而出" —— 两个长期独立运作但互相协作的集体，分别专注于幸存者支持与施暴者干预。

性侵、问责与同意权的议题由此席卷几乎所有无政府主义会议与集会。众多分销点开始销售相关主题的杂志，巡演乐队在舞台上公开讨论此事，其他城市的无政府主义者也相继组建了支持与问责团体。大型集会组织者开始制定应对方案，最终在2009年匹兹堡反G20峰会期间，构建起了完整的性侵应对体系。

那么，如今的情况如何？

诸如"同意"、"被点名"、"问责流程"和"施害者"等术语已被广泛使用，甚至沦为笑柄。大量人员因施虐行为遭到公开谴责，几乎任何时候都有数十起问责程序处于不同阶段的推进过程中。围绕"幸存者"与"施暴者"标签的身份政治已然形成，相关领域呈现两极分化态势。尽管各方努力警示风险并敦促问责程序参与者保持自我批判，但这些标签仍时常被用作权力杠杆 —— 既可赋予也可以剥夺合法性，亦可抹杀经验上的差异。

“费城挺身而出组织”持续开展工作，受高校委托推广其培训模式，并作为半正式的性暴力监督机构运作，全国各地的人们纷纷联系他们了解各类问责流程的最新进展。该组织曾在底特律美国社会论坛上与从事转变性正义工作的其他团体建立联系，并于2011年1月为社区问责制组织者举办了为期三天的培训。尽管其他城市的无政府主义者也尝试组建过众多类似的团体，但鲜有能与PSU比肩的持久性与影响力。随着圈内交流日益转向网络，若干网站（其中最突出的是anarchistnews.org）已成为围绕性侵与问责政治议题的口水战中心。同时也涌现出一些专门披露特定性侵施暴者信息的网络平台。

如今大多数无政府主义集会都会发布关于同意原则和性侵应对的指导方针，并常提及处于问责程序中的人的出席问题。基于2009年匹兹堡反G20动员中性侵应对组织者制定的政策，2010年华盛顿特区反IMF动员的组织者发布公告声明"不欢迎施暴者"。公告解释说，为保障幸存者在示威活动中的安全，禁止"曾实施侵害行为者、逃避问责程序者、以及拒绝遵守IMF抵抗网络同意准则者"进入所有组织空间及活动。近期，2012年多伦多无政府主义书展的组织者沿用了这种禁止所有施害者的措辞，并补充道：

> 我们理解并尊重各社区针对这些事件开展的自主处理流程。如果您已完成问责程序，且幸存者在社区支持下认为您已充分处理自身问题，则本声明不适用于您。

同样，2012年纽约无政府主义书展的组织者禁止以下人员参与：

> 曾实施过人际暴力、袭击和/或骚扰行为者， 除非 其正在积极参与问责程序，且当前完全遵守该程序的所有条款和/或要求（根据协调员、幸存者和/或被指定监督该程序所达成协议的人员的认定）。

引发主要争议的是对被指控性侵或虐待者实施的预先禁令。近年来，幸存者及其支持者日益要求禁止特定性侵者参与即将举办的活动。主办方在坚持相信幸存者与避免预判之间艰难抉择，同时还需要平衡透明度与隐私保护，避免造成二次创伤。当某网友公开纽约无政府主义书展组织者发给他的邮件时，网络舆论沸腾了—— 邮件要求其不要出席活动却未说明原因。有人将此解读为卡夫卡式的威权主义，认为这是通过匿名谣言预设罪责；也有人辩护称这是在保持中立的同时，为保障其他参与者安全所做的努力。

尽管针对性侵事件的应对方式争议不断，近年来无政府主义圈内的性规范已发生显著转变。同意权议题的讨论范围扩大了，性侵信息、幸存者支持及问责机制的可及性日益提升。这些变化明显改变了我们的性关系模式、身体认知方式及对幸存者的回应机制。相较往年，许多无政府主义者对性权力动态的认知更清晰了，在表达边界与欲望时也愈发自信。

然而，无政府主义社群中的施暴者有时会一边高谈阔论“同意与支持”，另一边行为上却一如既往。正如《无政府主义男性是我们的同志吗？》一文所质疑的：

> 问责程序常能带来很多好处，但有时它只是教会男性如何在言辞上伪装无害 —— 而其本质毫无改变。幸存者与朋友们只能困惑地猜测：这个男人是否不再构成威胁？最终，由于人们既不想显得过度敏感，又不知该采取何种进一步的行动，此事便逐渐淡出公众视野，施暴者得以在生活轨迹几乎毫无改变的情况下继续前行。

我们如何才能防止这些话语被机敏的性侵犯者所盗用？社区问责机制的存在似乎并没能改变其本应解决的行为模式。问题出在哪里？

[image]

社区问责流程的十大陷阱

需要说明两点重要前提：首先，这些陷阱源于实际运作中的问责流程 —— 基于我们的亲身经历。其中部分陷阱并非流程固有缺陷，而是执行者常犯的错误。面对诸多批评，有人或许会辩称："如果人们严格按设计实施模型，这些问题本不会发生。"

此言不假；但是，对于任何此类模型而言，要想具有广泛的相关性和适用性，它就必须足够稳健 —— 意味着即使在条件不理想、或者人们不能或无法完美遵循模型的情况下，也能取得成功。请谨记：这些陷阱并不意味着问责模型注定失败。恰恰相反，正因为我们致力于探索终结暴力侵害的途径，才必须以毫不妥协的批判精神审视相关实践。

其次，人们经常用来逃避责任的言论不应被误认为是问责流程的问题。例如："这些事让我们分心，偏离了真正的革命议题；制造分裂损害运动；追究责任是操纵/胁迫/过度强调/权力取"等等。这些并非问责机制的缺陷，而是父权制及其辩护者的症结所在。

话虽如此，以下是我们为了让彼此在无政府主义/激进派反叛者圈子内为性侵犯和虐待行为承担责任而开发的流程中遇到的一些主要困难。

1) 缺乏明确的终结标准，也无从界定成功或失败。

我们何时能断言某人已"处理好自身问题"？受害人及其支持者如何才能安心接受某人继续参与共同体活动？当期望不明确、目标不具体、评估时间线和方式不明时，所有相关人都可能陷入困惑和挫败。

这通常是因为我们对解决冲突和处理伤害的替代模式经验太少，以至于我们不知道该关注什么。例如，即便某人已"承担责任"，幸存者未必因此感到好转。这是否决定了过程的成败？如果当事人已完成所有要求，但他人仍质疑其采取的措施是否有效，又该如何确认真正的改变已然发生？伤害既成后，信任能否重建实属未知；如果无法重建，此类过程或许并非正确选择。

同样地，当何种程度的懈怠出现时，我们才能认定某人根本没有认真解决自身问题，从而停止徒劳的投入？某些问责流程会拖沓数月乃至数年，这毫无疑问会将集体精力从更有价值的领域中抽离。一个顽固的性别歧视者就足以破坏整个社群真诚推动问责的努力 —— 这恰恰说明，在流程拖垮所有人之前及时终止尝试是多么重要。

既然要投入如此多的时间和精力，我们需要一种方法来评估它是否值得，以及何时承认失败。

这要求我们明确失败的定义：例如将某人逐出圈子、尝试其他应对模式，或是向幸存者坦承无法满足其诉求。

2）成功的标准往往脱离实际。

例如，要求某人"解决自身问题"这类常见诉求，要么过于模糊而缺乏实质意义，要么实际上意味着一种深刻的心理转变，超出了能力范

围。正如《透彻思考施暴者问责制》一文所言：

> 施暴者问责绝非轻松速成的过程 …… 改变根深蒂固的行为需要终身承诺，需要持续的努力与支持。谈及后续跟进时，我们不仅要制定数周的计划，更应规划数月乃至数年的定期复查。唯有这种持久的支持，才能促成真正的转变。

坦率地说：如果要求人们为某个他们根本不喜欢的混蛋持续参与问责程序长达数年，并期望这种模式适用于越来越多的对象 —— 无论对方是否配合 —— 这根本不是一个现实的标准。

这并非否定文章观点；父权制与虐待行为模式的转变确实是终身课题。但当连无政府主义圈子里最热忱的理想都难以长久坚持时，我们未能持续这些漫长、困难、吃力不讨好的流程，又有什么好奇怪的呢？我们究竟能切实承诺什么？

3）我们缺乏实现诸多诉求的集体能力。

我们虽可宣称致力于满足幸存者的要求，但当这需要我们自己不具备的资源时，此类承诺不过是空洞的言辞。我们是否了解合适的反权威女权主义咨询师和治疗项目？当被指控者无力支付时，我们能否承担费用？面对不配合的人，我们能否强制执行意愿 —— 而作为无政府主义者，我们是否应该这样做？我们能实施哪些真正有意义的后续措施？在流动性强的亚文化圈中，我们能否切实承诺对某人进行长达数年的后续跟进、并建立持久有效的支持与问责机制？……

幸存者诉求与支持话语中常出现的一个词是"安全空间"，指幸存者能感到舒适并完全融入集体生活的理想场所 —— 这个永不可及的乌托邦。安全究竟意味着什么？这是我们能承诺的事物吗？从近期无政府主义聚会的政策来看，保障“安全空间”的主要方式似乎仅限于是排除曾伤害他人的人。但安全远不止于隔离那些破坏特定人群安全的人 —— 强奸文化与父权制渗透在我们生活的每个角落，它们绝非少数害群之马造成的后果。虽然排斥能让幸存者免于与伤害者共处的压力，也能保护社区成员免受反复施暴者的侵害，但这种排斥方式离真正的安全还差得远。事实上，我们依赖空间禁令，与其说是为了保障安

全，不如说是因为这是我们唯一能真正执行的安全措施。

在《安全是种幻觉》一文中， 安古斯蒂亚·塞莱斯特谴责了"安全空间的虚假承诺"：

> 我们无法为幸存者提供安全空间；在亲密友谊、部分亲属关系及偶发亲密关系之外，普遍意义上的安全空间根本不存在 …… 在父权制与资本主义的统治下，在性别歧视、异性恋霸权、种族主义、阶级主义（等等）的压迫中，安全空间纯属虚妄。我们越是试图营造社区层面的安全假象，当朋友和爱人遭遇暴力却得不到支持时，他们就越会感到失望与背叛。

对幸存者乃至所有人而言，真正的安全应该是什么模样？除了排斥与孤立，我们能否采取其他策略朝这个方向迈进？

[image]

4）我们缺乏咨询、调解和冲突解决方面的技能。

幸存者的诉求往往包括寻找咨询师或调解员。

要有效发挥作用，此人应具备以下条件：

- 愿意免费工作或按受助人的实际收入分级收费；
- 秉持反权威政治立场和幸存者意识的女性主义分析视角；
- 拥有足够的时间和精力可以长期积极地介入个案工作；
- 且需要与社区保持足够亲近以理解其规范，同时还不会直接卷入具体事件。

具备这些条件的人有多少？我们之中又有多少人连基础的积极倾听能力都欠缺，更遑论驾驭同意与侵犯的复杂动态、父权制条件反射、反权威冲突解决及心理转化的能力？而那些勉强符合或接近标准的人中，又有多少人尚未被繁重的事务淹没而不堪重负？

也许这是所有人的错，因为没有共同优先考虑这些技能。好吧，但是我们现在该怎么办？又该如何避免造成这样一种分工：让拥有某种技能或掌握某套行话的人在无政府主义版本的问责流程中变得类似于权威人士？

5）这类事务令人沮丧且高度耗费心力。

参与社区问责工作需要非常多的投入，情感消耗巨大，却往往得不到应有的认可或补偿。尤其当这些流程既难以维系社区完整性，又无法满足所有参与者时，更会让人精疲力竭且吃力不讨好。这项工作的沉重性令人望而却步，完全可以理解。

这并非意味着我们应将性侵与虐待的社区问责机制变得轻松愉快。但必须承认，这种机制本身构成了阻碍 —— 它让人们难以挺身而出，更难以长期坚守我们宣称必不可少的参与承诺。而当我们过度依赖圈内少数人的技能与经验时，这些问题将被无限放大。

6）问责流程吞噬了过多的时间和精力。

我们加入无政府主义阵营，绝非因为热衷于参与那些令人精疲力竭、永无止境的流程，去处理亚文化圈子里人们互相伤害的愚蠢行径。我们成为无政府主义者，是因为憎恶警察，因为热爱朋克演出，因为渴望更自由的世界，还有无数其他理由。当我们耗费大量时间精力解决内部冲突，说服顽固的性别歧视者为改变行为负责时，我们正冒着与最初凝聚我们的激情割裂的风险。

当我们连彼此间的侵犯都无法制止，更遑论粉碎国家机器、废除资本主义了，这种情况下大家就很容易对无政府主义政治观感到沮丧。这并非否定终结性侵与父权制度的革命性 —— 恰恰相反！但如果问责

机制 —— 尤其是那些令人沮丧且成效甚微的机制 —— 过度消耗了集体能量，我们既难以维系参与热情，更难吸引新力量加入抗争。

[image]

我们不能以虚假的团结为名掩盖暴力行为，压制幸存者的声音。这种旧有范式延续了压迫，削弱了整体效能。正是这种困境催生了社区问责机制。

我们必须找到应对暴力行为的途径，避免让它吞噬所有能量摧毁我们的斗志。

7) 亚文化纽带薄弱到人们轻易就能脱离。

须知社区问责框架所依据的许多非强制性修复性司法模式，是源自规模较小的原住民社群 —— 这些社群具有比当今绝大多数人能想象到的更加强烈的文化亲和力。主张应维护社群完整性、允许伤害他人者继续融入社群的理念，其前提是所有成员都对这个"社群"投入得足够深厚，足以承受问责过程中的审视与痛苦的情绪。

然而吸引人们投身朋克或无政府主义圈子的亲和力，往往不足以在成员感到被要求的行为威胁到自身时，将其牢牢扎根于此。被点名批评的人往往直接卷铺盖走人，有时甚至在被追责前就先发制人地离身而去。除非能联系到施暴者在新据点的社交关系网络（这种情况正日益普遍），否则我们几乎无力阻止这种逃避。当我们对拒绝问责者施加的主要惩罚仅限于排斥和孤立时，人们自然会通过逃离或退出圈子来规避这些后果。

8）集体规范助长并纵容不负责任的行为。

我们的个人选择始终发生在社会语境中，无政府主义圈子的某些集体规范助长了（即便不能说直接纵容）那些常导致越界和被公开指责的行为模式。

例如，在不少无政府主义圈子里，酗酒文化盛行，多数社交聚会围绕酒精和毒品展开。当人们过度饮酒或吸毒时，几乎没有防护措施，而那些自己想戒酒或减少大麻使用却又不愿失去社交生活的人，也鲜有替代空间可去。幽默和交谈规范强化了这样一种观念：醉酒是“正常”甚至有趣的，醉酒时人们的行为责任比清醒时更轻。一个又一个周末，我们营造出充满性暗示的空间，施加强烈的酗酒压力，导致人群因醉酒或药物作用而无法给予或接受明确的“同意”。当这些情境造成伤害后，我们却期待个人独自承担选择的后果，而非共同承担将此类行为正常化的集体环境责任。

当然，这些社会机制绝不能成为虐待的借口。但性侵行为发生于特定社会语境中，群体既可为社会规范助长的行为承担责任，亦可逃避责任。酒精与药物滥用只是群体规范纵容失责行为的典型例证。寻求问责者指出，其他阻碍追责的固有机制还包括：对圈内名人的偶像化崇拜（比如流行乐队成员、知名活动家等）； 认为性关系和恋爱关系属于"私事"、与外部无关的观念；以及认为遭受系统性压迫的群体（如酷儿群体和有色人种）不应"家丑外扬"，以免被进一步妖魔化的信念。

[image]

我们是否愿意在集体层面审视并挑战群体规范，探究这些规范如何助长或抑制问责行为？

是否有可能以某种结构化的方式让整个圈子集体承担责任以追究我们纵容或原谅的行为？

结构化方式追责很可能使我们当前在个人问责过程中遭遇的所有问题倍增，但是，如果不承认并挑战集体责任，仅追究个人责任终将徒劳无功。

9）对抗性司法体系的残余影响正侵蚀着我们对社区问责模式的应用。

针对问责制最尖锐的抨击，往往指向其“伪司法”性质。

一方面，伤害他人者鲜少经历除权威体系外的问责机制；此类尝试常被指责为"猎巫行动"、"威权主义"、或“警察/法官/律师/狱警式行径”。昔日的反政府激进分子往往上演惊人转变，突然对政府承诺的"正义" 产生了浓厚兴趣： "无罪推定去哪儿了？我难道不能获得公正审判吗？不能为自己辩护？听听我的品格证人的证词啊！"

另一方面，追究责任的人也同样受制于对抗性冲突解决模式的条件反射，尤其面对顽固不化的强奸犯时，极易陷入这种框架思维。

甚至有些参与者 将问责程序当成了威胁手段或权力杠杆 。虽然这种行为或许能理解 —— 毕竟在遭受虐待和侵犯后人们常会感到挫败和无力 —— 但它毫无疑问 会破坏 寻求非对抗性解决方案的努力。

一份公报揭露了激进派反叛圈子内的问责程序未能摆脱政府法律体系逻辑的致命缺陷，该公报解释了一群女性为何对性侵犯者采取肢体对抗：

> 我们出于纯粹的必要性做了必须做的事。作为激进派反抗者，我们深知政府的法律体系根深蒂固的荒谬性 —— 诸多法律与司法程序充斥种族主义、阶级主义、异性恋霸权主义及厌女症。替代性问责机制与传统体系如出一辙，往往迫使幸存者重温创伤，更要求她以自己的声誉（这个概念本身就充满问题）作为可信度的"证明"。这些机制终究只是政府司法程序的无效复刻：施暴者继续逍遥法外，而幸存者却要终生背负性侵记忆。无论是国家法律体系还是社区替代问责机制，都远不足以保障幸存者的权益，更谈不上具有革命性。

[image]

10）性侵问责的措辞与方法被应用于并非其初衷的情境。

此类误用的典型案例，是广泛采用危机干预幸存者支持原则中"始终相信受害人"条款。

这在危机干预组织的语境下完全合理 —— 这些机构只专注于向经历过一种普遍不被相信的创伤形式的个体提供情感支持和服务，而获得信任对康复过程至关重要。但如果以此作为冲突解决基础则不合逻辑。在危机干预咨询环境中，或当信任的朋友向您倾诉以寻求支持时，焦点应该始终放在幸存者的需求上；但转变性正义要求兼顾所有相关方的需求 —— 包括施暴者 —— 从而考量各方经历和视角。

这并非要求我们辨别谁说真话谁撒谎 —— 那仍然是对抗性司法体系的残余；亦非主张所有观点等值而无人对错。其真谛在于：要促使当事人承担责任，我们就必须愿意接纳其当下的处境，这意味着承认个体经历可能存在显著差异。承担责任的前提是需要承认自身犯错的可能性，至少要意识到他人可能以截然不同的且感觉充满伤害的方式经历同一事件。但如果完全由幸存者定义现实运作规则，则可能不利于这种模式的社区问责。

性侵问责话语过度使用和误用的另一例证，是人们将非性侵行为也纳入到问责程序中了。例如当非虐待性关系破裂后（即普通分手），如果一方感到愤怒受伤，便可能倾向于通过指责对方并要求问责来表达不满。这种诉求可能表现为要求将某人逐出特定空间 —— 借用这种常见问责手段的威慑力。

人们因各种原因感到愤怒或受伤时，渴望通过将自身痛苦愤怒包装成要求"问责"的指控来获得即时情感认同（某些圈子里确实如此），这种心理可以理解 ——无论这种流程和话语是否适用于此种情境。

这种做法的危险之处不仅在于这些术语和策略本来仅适用于特定冲突类型而非其他情形，更在于，过度使用会使其失真，导致人们轻视那些本应该被严肃对待的侵犯与虐待事件 —— 正是为应对此类事件才创立了这些机制。令人欣慰的是，性侵犯与虐待议题已广泛进入激进社群的讨论范畴。但我们必须警惕：切勿将针对特定冲突与压迫行为制定的应对方法，泛化应用于并非为之设计的其他情境。

某些情况下，因他人的不当行为而感到沮丧的人甚至不愿指出问题，生怕对方被贴上"施暴者"的标签，或担心周围其他人将伤害程度较轻的非自愿行为视为性侵犯，从而将指出问题者视为"幸存者"。当性侵问责话语的过度使用，与围绕幸存者/施害者的身份政治及"施害者禁止入内"等政策相互交织时，本应促进问责的努力反而可能导致人们不

敢对其他糟糕行为发声 —— 只因害怕某人会被永久贴上"施害者"的标签，而非通过几次对话、道歉和阅读一本小册子就能解决问题。

[image]

新方向与后续问题

那么我们该何去何从？人们对问责机制普遍感到幻灭，这表明我们已陷入了僵局。

本文提出四条可探索的途径 —— 与其说是解决这些困境的方案，不如说是用于实验的方向，以检验它们能否开辟新路。

方向一：幸存者主导的自发维权

> "我想复仇。我想让他体会那种失控、恐惧与脆弱 —— 正如他曾让我感受的那般。性侵之后，安全感终究是幻影，但施害者必须承担后果。"—— 安古斯蒂娅·塞莱斯特《对问责制的反思》

2010年，纽约与圣克鲁斯两地发生女性团体围堵知名无政府主义男性的事件，在无政府主义圈层引发轩然大波。围绕这些行动展开的讨论揭示出，无政府主义圈层普遍对现有性侵应对机制感到沮丧。

肢体对抗并非新策略 —— 在社区问责机制尚未普及前，这本就是幸存者应对施暴者的方式之一。随着问责制的发展，许多人因其未能阻止强奸或保障安全而摒弃肢体对抗。幸存者主导的私刑行动伴随着批判问责流程的声明，折射出幸存者在现有方案徒劳无功时所感受到的无力与绝望 —— 他们正竭力寻求替代方案。

然而，无论是否存在其他选择，幸存者主导的自卫行动都是应对性侵犯的有效方式。人们无需感到无力或认为其他选择徒劳无功，即可对施暴者采取果断的肢体行动。

这种方式具有多重优势：首先，与许多问责程序截然不同，它设定切实可行的目标并能成功实现。相较于漫长的、反复触发创伤且过度抽象的程序，这种方式更能赋予力量并带来满足感。女性可通过对抗建立集体力量，推动其他协同的反父权行动。肢体对抗传递着明确信号：性侵不可容忍。如果性暴力将父权制烙印在女性身体上，那么复仇就体现了女性的抵抗。

最重要的是，这种行动无需中介 —— 正如《幸存者自主权与暴力札记》的作者所言：

> 对各种问责流程的普遍批评是，它们倾向于模仿某种司法系统 —— 通过结构化调解实现某种形式的改造或惩罚。尽管幸存者主导的结果绝非等同于国家强加的裁决，但过程本身仍是调解。反之，摆脱司法框架意味着拒绝调解机制 —— 这种机制残留着"人际互动必须由第三方引导"的观念，即便第三方是我们自己选择的。因此，对施暴者的攻击是直接而无中介的，恰恰是任何司法体系所禁止的；欲望与行动之间的界限就此消弭。

当然，私刑行为也存在诸多弊端。选择升级冲突将带来法律和人身的双重风险。警方更可能以"群殴"罪名起诉冲突双方，而非"涉嫌"性侵。正如受虐妇女权益倡导者所知，伴侣暴力极易演变为致命危机 —— 女性死于伴侣之手的比例远高于其他类型施暴者。

除了即时风险，正如俗语所言，暴力无法修复社会关系；扼杀某个卑劣之徒，无论对伸张正义的幸存者来说多么痛快，都无助于提升安全感、更无法终结制度性强奸文化 —— 如前所述，正是这种在应对个案时直指强奸文化根源的诉求，才催生了社区问责机制。

更存在着非受害人负责的私刑传统 —— 这种男性暴力已被众多幸存者与无政府主义女性揭露，其本质是满足男性自恋而非促进治愈和安全。男性幸存者盟友刊物《支持性侵幸存者》在探讨"零暴力原则"时，对此现象提出了尖锐批判：

> 痛揍强奸犯的屁股就能让强奸不曾发生吗？他的痛苦能消除幸存者的伤痛吗？幸存者需要去安抚另一个失控的暴力男人吗？答案很可能都是否定的。
>
> 鉴于绝大多数性侵案件（据称超过99%）由非跨性别男性实施，支持幸存者的男性更需深刻认识男性暴力的影响。正是男性暴力导致强奸，而非终结强奸。你们的行动必须致力于终结男性暴力。
>
> 我们无权代表幸存者 —— 尤其是女性幸存者 —— 对强奸事件的反应方式。如果女性作为幸存者主体，选择以暴力或要求男性支持者参与暴力作为集体回应方式，这应由幸存者自行协商解决。但对于支持幸存者的男性而言，必须摒弃男性复仇的冲动，切断男性暴力的循环……你既无责任也无权利以私刑者姿态介入并擅自处置。

这种批判促使明尼阿波利斯的DWOS等团体将"非暴力"确立为原则。需注意的是，该批判刻意不适用于幸存者主导的自卫行动，而是针对不负责任的非幸存者反应。

那些被幸存者主导团体攻击的无政府主义男性的辩护者声称，私刑具有威权性质："问责不能是单向的，否则就成了惩罚和警察权力的同义词。" 但正如幸存者公报所阐明的，私刑并非"问责"的形式—— 至少不是无政府主义圈内普遍理解的、基于转变性正义的社区问责；相反它是对这种问责的明确拒绝。它并非伪司法程序；它拒绝国家与非国家层面的冲突解决机制，主张对伤害采取直接的、无中介的回应。无论我们是否认同其正当性，都不应将其误解为问责机制的失控。恰恰相反，这是对现有问责机制失败的刻意回应。

[image]

只要我们针对性侵与虐待的问责实践未能切实满足民众需求，私刑行为就会持续存在，这将不断挑战无政府主义者对转变性正义的倡导，迫使他们将理想转化为现实。

我们究竟该致力于建立足够有效的问责机制以消除私刑的必要性？还是应当发展并推广幸存者主导的直接对抗实践？

[image]

方向二：通过性别组织实现预防

这点显而易见却值得强调：与其耗费大量精力思考如何支持受害者并应对施暴者，不如将重心放在预防暴力行为本身，岂非更合理？

当然，说起来容易做起来难。但迄今为止，我们讨论的仅是针对伤害形式的事后反应机制 —— 即便在探索更优应对方案时，我们仍默认这些伤害将持续存在。

借用非营利性强奸危机中心的术语体系：应对侵害行为及通过问责程序处理施暴者，属于干预措施或三级预防范畴。一级预防是指通过教育并改变社会、文化和制度规范来阻止初次侵害行为；二级预防聚焦识别与侵害相关的风险因素并加以干预以防事态升级。因此当无政府主义社群中性侵事件持续发生时，我们不应简单判定问责机制之类的应对措施失败，而应在维持现有干预的同时拓展预防工作的广度。我们究竟该如何从源头杜绝这些事件？

在无政府主义圈子之外，性暴力预防工作通常聚焦于教育：针对女性开展自卫与伤害减免相关的培训；针对男性破除强奸迷思并承担终结男性暴力的责任；面向全体人群培养健康沟通和构建关系的技巧。在无政府主义圈内，部分女性组织了自卫技能分享活动，围绕同意权、伴侣沟通及积极性观念展开的大量大众教育（主要由女性主导实施）已取得成效。如前所述，这些举措显著改变了无政府主义者的性话语体系，但要打破根深蒂固的模式，我们需要更深入地介入性别压迫议题。

实现这种深刻转型的路径之一是通过性别集体组织，特别是专注于改变男性对性与同意态度的男性团体。然而除明尼阿波利斯的DWOS、费城男子集体及《社会解毒》杂志等少数例外，近年来无政府主义者群体中鲜有反性别歧视男性组织的可见踪迹。过去某些圈层中，反性别歧视男性团体曾与自主女性组织结盟。如今这类组织形态已式微，

原因包括反女权主义的反扑、将所有基于性别的组织视为本质主义问题的跨性别和酷儿政治认知，以及众多跨性别的反父权激进分子投身性侵应对与问责工作。如组建反性别歧视男性团体，与自主女性组织协同开展性侵预防工作，能否成为值得探索的新方向？

这种方法可能带来多重优势。建立分享瓦解父权制和自我蜕变技能的机制，既能减少参与者的问题行为，又能为伤害他人者提供问责响应的基础架构。现有的男性团体使人们能够主动承担自我教育与反父权行动的责任，无需依赖"施害者"标签或外部"要求"。人们可因各类行为被转介至团体 —— 这些行为单独看或许不足为奇，却可能是潜在父权模式的预警信号，从而让他人能在这些模式演变为更严重的危害前介入（即二级预防）。终于，我们有了一个能为那些希望"解决自身问题"的人提供支持的场所，无论他们是出于社区压力还是自我驱动力。

但男性团体不仅处理问题行为，更提供深化关系、学习成长、政治觉醒、情感联结乃至娱乐的空间。这种多元价值应能激发参与热情并维持持续的投入，因为它并非仅聚焦于令人精疲力竭的危机模式问责工作。这些团体开展的学习、反思与关系建设，能强化无政府主义场景中其他激进组织的工作，使我们在危机时刻拥有更多的选择、技能和行动力量。与许多内向型社区问责策略不同，男性团体能与非无政府主义者及团体互动，传播反父权信息与实践，同时借鉴其他女性主义组织经验，使我们的行动与更广泛的社会抗争 —— 反对性别暴力和父权制总体战略 —— 产生关联。

但等等…… 性别问题该如何处理？在当前北美无政府主义圈的性别政治语境中，任何基于性别的组织形式都只会被视为可疑。这难道不是陈腐身份政治的残余、左翼愧疚的遗迹、过时的本质主义，以及可疑的威权实践吗？我们不正是要摧毁性别二元制——父权制与性别压迫的真正根源吗？基于性别（或指派性别等）的组织形式，岂不是在强化我们试图推翻的父权制与跨性别恐惧框架吗？

在界定何谓"男性"时，确实存在诸多棘手问题：无论是基于自我认同、社会认可还是出生性别认定，不同性别酷儿与跨性别者的归属如何界定，以及如何厘清个体经历了何种社会化过程。要终结一切形式的等级制度与异化，需要比身份政治更具解放性的策略。但现实情况是：基于性别的压迫行为与权力模式仍沿着性别界限呈现高度可预测

的分布。如果基于性别的组织形式能打破这些模式，或许我们必须接纳这种矛盾，并竭力应对其错综复杂的现实。

除原则层面的性别化组织问题外，此种策略还存在其他潜在困境。我们无需认同所谓"良善无害的无政府主义男性"存在 —— 毕竟性侵者才是真正需要警惕的对象 —— 但必须承认：那些最需要审视自身性别歧视行为的人群，往往也是最不愿参与此类活动的群体。此外，参与正式男性团体可能成为性别歧视者获取合法性的途径 —— 当被指责时，他们挥舞着女权主义盟友会员卡转移公众对其恶劣行为的关注。如果基于性别的组织形式使男性团体（即便反性别歧视的团体）凌驾于女性和/或跨性别者的自主组织之上，这反而会巩固而非挑战特定场景中的父权权力关系。

[image]

方向三：不只是问责，更是解决冲突

我们在追求问责方面的努力之所以受挫，是因为我们几乎没有解决内部冲突的模式、方法或技能。

尽管我们投入了大量精力制定应对侵犯与虐待的策略值得称道，但还有无数其他类型的冲突和有问题的行为同样需要工具来处理 —— 如你所见，针对性侵犯的问责方法在不同情境下并不适用。

[image]

如果我们优先培养冲突解决和调解的技能呢？

当然，存在性侵和虐待相关的特定议题，这些议题不应在普遍的冲突解决框架中被忽视。但如果我们能建立处理各类冲突与伤害的先例、话语体系和技能库，让参与冲突解决流程成为常态且不再令人畏惧，那么当得知自身行为伤害他人时，我们或许能减少防御性反应。

[image]

与其延续"幸存者"与"施害者"的身份政治，我们更应创造既不美化也不

妖魔化他人的细腻话语体系，要求所有人持续参与终身的自我蜕变。

这需要对造成伤害者同样怀有同理心，为他们创造承认行为并获得治愈的空间。

将性侵问责置于更广泛的冲突解决框架有何优势？

1. 将无需通过定义层级或试金石来判定何为"严重侵犯"。

1. 通过建立集体参与低强度冲突的先例，我们能积累应对危机的宝贵经验。

1. 将冲突解决定位为集体责任，可避免形成专职调解人员阶层，并更易物色与事件保持足够距离、能中立调解的支持者。

需特别强调：调解不适用于多数伴侣虐待案件。《反思施暴者问责制》一文阐明：

[image]

调解不应替代问责程序。

调解适用于双方存在需解决的冲突的情形；而虐待行为并非双向。

虐待问题绝非单纯需要双方坐下来协商解决。

调解员固然可在问责程序中协助推进具体协商事项，但请勿将调解会谈作为替代长期问责程序的选项。

为家暴幸存者提供咨询的专家们都知道，在伴侣存在明显虐待行为的情况下，不应进行"伴侣咨询"，因为施暴者通常会操控咨询过程，导致关系中潜在的虐待性与不平等动态问题得不到解决。这一点至关重要，必须谨记避免将冲突解决框架套用于虐待性关系的情境。

其他弊端呢？的确还有一个问题：我们常被要求采用超出自身能力或资源的解决方案来应对现有困境。在学习冲突解决技巧的长期过程中，我们该如何应对？

- 幸存者可能因暴力行为被归类为“强度较低”或“政治意义不大的冲突”而感到挫败，这会淡化他们遭受的伤害。
- 要求幸存者在面对施暴者时使用温和措辞，可能强化"幸存者有过激反应"的指责论调，暗示性侵犯“不足以被强烈谴责”。
- 此外，男性"冲突解决专家"可能劫持幸存者支持工作，使其偏离女权主义焦点。

我们必须承认性侵犯与虐待的特殊性，尊重幸存者的痛苦和愤怒情绪，在拓展冲突解决范畴时，务必考量压迫性权力结构的存在。

[image]

方向四：同心圆式的亲密圈

> 在激进社群中根本不存在问责机制，因为所谓的“社群”根本不存在 —— 至少在性侵与虐待问题上如此。如果进行一次诚实的调查，你就会发现我们根本无法达成共识。在此语境下，"社群"不过是个被频繁援引却屡遭滥用的神话术语。我再也不愿为此投入心力。
> —— 安古斯蒂娅·塞莱斯特《关于问责制的反思》

所有这些问题的核心都存在一个未解之谜：何为"社群"？我们作为无政府主义者共同存在于其中吗？作为朋克青年呢？作为特定地方场景的参与者呢？就因为我们身处同一场抗议、演出或群众动员？我们是主动选择加入的吗，还是无论认同与否、无论喜好与否，都身处其中？而这一切又由谁来决定？

没有社群就谈不上社群问责。如果缺乏对社群内涵的清晰认知，整个

转变性正义框架就会分崩离析。

但遗憾的是，似乎没有人能为我们所处的环境解答这个问题。在缺乏答案的情况下，我们不断撞得头破血流：当恶劣的施暴者被揭发后逃离城镇或消失于圈子时、当某些人凭借自己在圈子中的权力地位操纵圈子边界以排斥幸存者和盟友时 …… 这绝非抽象问题：它关乎我们行动的本质，关乎权力在圈子中的运作方式。

社群通过具体机构而得以具象化——北美无政府主义圈由网站、聚会、社交中心和集体住房构成。尽管无人点名（联邦调查局或许例外），且我们常争论谁才算真正的无政府主义者，但穿行于这些空间的人们仍能感受到归属感。我们通过共同实践编织这种归属感，这些实践将我们标记为“战友”：服饰与身体改造（[image]匿名着装 ）、饮食卫生习惯、带有专业术语和文化参照的对话。

但仅仅“属于”无政府主义"圈子"，是否足以支撑问责策略所要求的社群形态？我们能否将这些模式切实应用于我们这些离散的、碎片化、大多非结构性的“不合群”松散联盟？

当我们在人生旅途中穿梭于朋友、邻里和同志的联结时，我们既不属于单一的整体社群，也不能仅仅算作多重社群的网络。相反，我们与他人的关系呈现为同心圆式的亲密圈层。由此，我们可以勾勒出一个初步的模型，来构想如何将社群问责机制应用于无政府主义圈子。

我们对无政府主义社群的认知存在一个主要缺陷在于其往往基于隐含和默认，而非明确阐述。除特定的项目或集体外，我们很少直接表明对共享各类"社群"的同伴所作的承诺与期望；例如，室友共同生活时，会约定按时缴付账单、清洗餐具并尊重彼此空间。倘若我们将这种明确意图延伸至所有战友关系呢？这显然不现实：难道要我们与全国（甚至仅仅是我们所在的城镇）的每位无政府主义者坐下来，逐条列明彼此互动的明确标准与相互期待？

当然不可能…… 而这恰恰是关键所在。既然无法实现，我们就必须探索如何在生活中不同关系网络中集体确定这些准则。

[image]

与其假设存在某种"共同体"，并试图依据这种虚构概念追究责任，倒不如在各个亲和圈层中明确彼此的期望与承诺，以此作为应对冲突和伤害的基准。

例如，假设我的核心圈层是我所在的亲密团队。这些都是我最信任的人，我愿与他们共担风险，为他们付出一切。在化解冲突与处理伤害时，我对这群人的信任度远超任何其他人。在此模式下，我会与亲密群体预先商定应对机制 —— 从最轻微的分歧到最严重的伤害，都将纳入讨论范畴。这如同朋友与战友间的事前协议，为可能出现的状况预先铺垫。这样，当我的伙伴们伤害我时，我便清楚该如何应对，同时为长期协作的转变过程奠定共同信任的基础。

虽然我不会将这种信任延伸至多数人，但在这个群体中，我们共享着深刻而明确的亲和力，因此我愿意接受批评、直面问题并推动转变 —— 也相信我的同志们同样如此。

这种核心亲密圈的其他范例可能包括：家庭/家族（血缘或选择）、房屋与土地项目、各类集体组织，或是紧密相连的朋友圈子。

第二层圈子可能是共享的社区空间，比如信息站或社交中心。这是一个相对稳定的群体，其中有些人我比较熟悉，另一些则不那么熟悉，但这里也是开放空间，可能会有陌生人前来。由于并非完全固定的群体，且并非每个人都能或愿意达成直接的协议，因此可以围绕尊重、同意、反压迫、资源使用等事项建立集体共识。这些约定不必具有权威性，可由集体决定，并随时由受影响最大群体同意修订，且无人被迫遵守；无法或不愿遵守者可选择退出该空间。因此，只要当事人仍愿参与该空间，我便愿意配合追究其责任。

既然定义我们"共同体" —— 即彼此具备亲和关系的纽带 —— 正是我们共同参与该空间的体验，那么当某人停止参与时，我们便不再构成共同体，自然不应期待通过该共同体追究或要求他人承担责任。相应地，如果有人违反或拒绝遵守集体标准，则存在既定程序可追究其行为责任；如其拒绝配合，他人可基于良知将其排除于空间之外。

此类圈层的其他范例包括特定活动、大型组织项目，及在共享社交空间中松散聚集的人群。

这种同心圆式的亲和圈子框架可帮助我们思考如何在无政府主义者群体中最佳实践近年来探索的问责制。当圈层向外延伸至大规模群众动员、"无政府主义者"、"朋克"、及更广义的激进派"社群"时，具体界定社群范畴并在其中落实问责制便愈发困难。我们无权要求任何人基于所谓的共同理念向我们"负责"。缺乏实质基础的"社群"既无激励手段也无强制力 —— 既无法奖励配合者，亦无法胁迫他人就范。因此，当某个自称无政府主义者的陌生人实施性侵时，如果试图以社群问责制来应对这种情况，恐怕并不现实。

那么我们该怎么办？报警抓人？痛打一顿？把他们赶出所有同道掌控的机构？又该如何应对那些离开一个场所后转而又在另一处重蹈覆辙的反复作恶者？……我们没有明确答案。

[image]

但必须在每个亲密圈中展开讨论 —— 在危机迫使我们仓促应对之前，就该明确行动准则、处理伤害和化解冲突的机制。

除非每个集体、空间、社交团体及其他无政府主义组织都彻底落实这些机制，否则我们根本无法指望以正式的社区问责制作为解决问题的策略。

组建亲密团队是无政府主义组织工作的关键环节。它可以简单如召集朋友共同行动，也可严谨到您能想象到的最正式的组织架构。其核心价值在于守护无政府主义的根本原则 —— 自愿结社，即我们能与任何人自由行动，不受胁迫或官僚体系的束缚。这个简单过程构成了我们示威和动员行动的核心，但或许我们可以借此来构想整个无政府主义社群及其环境。如果我们能建立更紧密的联系，更具体地理解彼此间的亲和关系，或许就能为将社区问责从模糊争议的梦想转化为现实奠定基础。

[image]

结语

希望本文能促使无政府主义者反思自身真正的亲和力所在。或许通过尽可能明确彼此的期望与承诺，我们能规避迄今为止在问责制实验中遭遇的诸多陷阱。我们还可考虑拓展幸存者主导的自卫行动，推动反性别歧视男性团体及基于性别的组织建设以瓦解强奸文化，或扩大对冲突解决与调解的关注。

无论选择何种路径，无政府主义者都必须竭尽所能打破圈内虐待与侵犯行为的僵局 —— 我们的解放正取决于此。

附录

参考文献

- "An Internal Action of the Vaginal Liberation Front", in *Men in the Feminist Struggle*
- "Don't Believe the Hype"
- *Fight Rape! Six Years of Men's Group and Accountability Work* by Dealing With Our Shit
- "IMF Resistance Network Consent Guidelines: No Perpetrators Welcome"
- "i. communique" by Radical Women's Kitchen
- "Is the Anarchist Man Our Comrade?"
- "Kafka sales will be through the roof at the NYC Anarchist Book Fair"

- “Notes on Survivor Autonomy and Violence”

- “Safer Space Policy,” by NYC Anarchist Book Fair Collective

- “Safer spaces, false allegations, and the NYC Anarchist Book Fair”

- “Safety is an Illusion: Reflections on Accountability” by Angustia Celeste, in *It’s Down To This: Reflections, Stories, Critiques, Experiences, and Ideas on Community and Collective Response to Sexual Violence, Abuse and Accountability*

- “Sexual Assault and Consent Policy” by Toronto Anarchist Book Fair Collective

- *Supporting a Survivor of Sexual Assault* by Men Against Rape Culture.

- “Thinking Through Perpetrator Accountability,” in *Rolling Thunder #8*

- “We Are All Survivors, We Are All Perpetrators,” in *Rolling Thunder #1*

书

- *The Color of Violence: The INCITE! Anthology*, by INCITE! Women of Color Against Violence

- *The Revolution Starts at Home: Confronting Partner Abuse in*

Activist Communities, edited by Ching-In Chen, Jai Dulani, Leah Lakshmi Piepzna-Samarasinha and Andrea Smith

- *Instead of Prisons: A Handbook For Abolitionists*, by Prison Research Education Action

- *Peacemaking Circles: From Crime to Community*, by Kay Pranis

小册子

- It's Down to This: Stories, Critiques and Ideas on Community and Collective Response to Sexual Violence and Accountability

- What Do We Do When #2 and #3

- An Activist Approach to Domestic Violence

- Thoughts About Community Support Around Intimate Violence

- See No, Speak No, Hear No

- Alternatives to Police by Rose City Copwatch

- Learning Good Consent

- Support

- World Without Sexual Assault

- Let’s Talk About Consent, Baby
- Our Own Response
- A Stand-Up Start Up: Confronting Sexual Assault with Transformative Justice
- Beautiful, Difficult, Powerful: Ending Sexual Assault Through Transformative Justice
- Conflict Resolution Circles
- As If They Were Human: A Different Take on Perpetrator Accountability
- Revolution in Conflict: Anti-Authoritarian Approaches to Resolving and Transforming Conflict and Harm
- For a Safer World

其他资源

- Creative Interventions Toolkit
- Toward Transformative Justice, by Generation Five
- Community Accountability Principles/Concerns/Strategies/Models
- Community Accountability Within People of Color Progressive Movements

- Hollow Water (documentary film), by Bonnie Dickie
- Ideas, Actions, Art, & Resources for Communities Responding to & Transforming Violence
- Conflict Resolution Information
- Restorative Justice Information Clearinghouse
- International Institute for Restorative Practices
- *Policies for Mass Mobilizations around Sexual Assault and Consent:*
- Sexual Assault Disclosure
- Responding to Sexual Assaults at Mass Mobilizations
- Example Consent Policies

[image]
[image]

恢复团结：超越米兔S09E02

[image] 关键词	关系结构 内讧 团结 性关系 性暴力
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会 ；
[image] 创建时间	2025年1月3日
[image] **Description**	关系结构革命

华人异议圈子内曾经和现在出现的所有矛盾、冲突、错误和危险，从未超出过历史上的激进派社群中发生的状况，并且直到如今累计起来也仅仅是历史上曾发生过的千万分之一。

本文以美国反抗社群的近代历史为例，不仅希望说明具有同样经历的前辈们参加如何处理同类事件，并且希望引发思考，关于作为今天的新生力量的我们如何有望青出于蓝。

- Table of Contents

  摘要
  引言
  初识"问责制"
  方法论
  篇章组织形式
  第一章 场景铺陈：激进左翼亚文化
  作为激进左翼亚文化
  亚文化作为颠覆性存在
  行动者亚文化
  亚文化中的文化内核
  内部等级结构
  作为激进左翼社会运动

预示性政治
准入与网络
团结
关系与性
权力、文化与实践
布迪厄的分析框架
将布迪厄理论应用于亚文化和社会运动
社会运动中的社会公正文化
第二章 方法论
历史背景
该场域的当代文化
朋克
人口统计数据
访谈
小册子
性别歧视主题杂志标题（符号表示实体书^或PDF*）
同意与性侵犯主题的小册子（符号表示实体书^或PDF*）
男性团体主题小册子标题（符号表示纸质版^或PDF*）
转化性正义与问责制杂志标题（符号表示纸质版^或PDF*）
第三章 新左翼运动的历史模式
学生非暴力协调委员会（SNCC）
SNCC的组织与领导
SNCC内部关系
性别、种族与内部纠纷
黑豹党
黑豹党中的性别问题
黑豹党中的性关系
内部争端和自我批判
争取民主社会学生组织（SDS）和地下气象组织（WUO）
领导层架构
关系与性
问题、批评与自我批评
社会运动中的模式
第四章 组织、性与关系
组织中的性别问题
领导力
会议与共识

分工
直接行动
性中的性别
性关系
物化与“把妹活动家”
知情同意
问题优先级
安全文化
革命之后
第五章 转化性正义与问责机制
预防性措施：安全空间
激进主义者的“更安全的空间”
复杂性与局限性
批评
问责制
转变性性正义之前
修复性与转化性正义
作为行动主义中的问责机制
三大组成部分
A 幸存者
施害者
社群
问责流程
诉求
分离
准备工作
调解人
会面
第六章 发展与后果
社交资本与权力
谁能获得信任
以幸存者为中心
拒绝参与和漠不关心
复仇与权力
公开谴责
文化资本与暴力
预防与恐惧
文化规范与暴力
反情报计划、警察管制与国家机器
实践和成效

DIY流程
官僚主义
定义“成功”
社群与可持续性
其实并没有社区
破碎的社群
行动主义的转变
离开社会运动
结论
分析与实证发现
亚文化中的预示政治
刑事司法的替代方案和矛盾
混合性别运动中的女性主义政治
可能的解决方案
研究意义
问责制与转变性正义的未来

[image]

米兔是怎么来的？
它为什么曾经重要？
又为什么后来快速失败？
我们被什么干扰了吗？
还缺少什么？
或者，我们的战术策划是否一直不够充分？……
最重要的是，接下来如何升级它？

摘要

在激进左翼活动家亚文化中，"问责程序"是一种处理虐待和性侵犯的DIY转变性正义形式，其核心在于满足"幸存者"的需求并促使"施害者"的转变。

在行动主义革命派圈层中，识别虐待行为尤为困难，因为这意味着必须承认被视为“政治上高尚”之人的不当行为。流程的具体实施细则具

有情境性和权宜性。最普遍的模式是男性身份认同者对女性身份认同者、非二元及跨性别者的侵害。本研究探讨活动家们发展这些流程来解决问题的动机，以及它们是否成功。

在亚文化圈内，该议题的重要性足以催生研讨会、培训课程、教学体系，值得花费大量时间，形成专项小组，甚至终结社群。然而，这种重要性并未/尚未在学术界得到体现。

作者访谈了12位以幸存者、施暴者/加害者、协调员/调解员、或普通支持者身份参与其中的活动家；此外还从121份独立刊物中收集补充资料，分析围绕性别歧视、同意权、男性团体及转变性正义的实践经验。

发现的问题包括：活动家在青年亚文化中采用基于社群的策略、创建灵活社会机构替代方案的复杂性，以及围绕性别平等发展符合预示性政治实践的文化规范 —— 尤其在活动家彼此之间不可避免的性关系中。所有这些问题都汇聚于一个人员流动性很高且不稳定的亚文化群体，在此活动家们并没有完全与主流机构及文化实践切割。

活动家的行话包含反思性与特权概念，但承认过错并承诺改变并非我们文化范式的一部分。主流文化 —— 正如政治领域和“米兔”运动所示 —— 已证明否认过错对个人是有益的。在"问责流程"中，即便发生转变也鲜少被认可。如果活动家追求团结，就不能纵容不公，被边缘化的人也不应继续被边缘化。

[image]

引言

尽管由各种团体构成的结构具有可塑性，但共同的社会、意识形态和文化实践确立了可辨识的激进社会运动亚文化的存在。各类团体、组织、个人及场所构成了密集而广阔的网络，旧团体解散，新团体涌现，彼此间的界限逐渐模糊。个人常具有多重团体成员身份，通过组织活动、友谊、也包括性关系，相互联结。活动家们自称为"社群"成员，以此传递相互依存的意识并强调团结精神。尽管这些群体不使

用"亚文化"标签，但在主流文化语境中仍展现出独特的文化特征。

激进活动家们怀有共同目标：对抗被视为社会问题根源的既有权力结构。无政府主义、反资本主义、反种族主义、女权主义、酷儿运动等左翼激进团体虽理念未必完全一致，却存在思想意识形态的连续性。大家都认识到社会问题植根于现代政治/资本主义体系，是该体系为少数人维系特权和权力的产物。激进左翼认为，改革，尤其是通过主流、体制化和非营利组织进行的改良，维持并加固了不平等，改良仅提供了临时性的解决方案，尤其是它消解了剧烈的社会变革的可能性。诸如"团结而非施舍"的口号，正是对既得权力财富阶层居高临下态度的批判。他们质疑制度化目标本身及其实现手段的正当性。

政治理念在日常生活中的实践往往不够精准，而运动内部对团结精神的强调，可能模糊了女性、非二元及跨性别者面临的复杂处境。人际互动机制以及融入激进左翼社会运动的议题，鲜少成为研究焦点。本论文的认识论根基植于社会运动与文化研究领域。依托这些学科及皮埃尔·布迪厄的理论框架，本文研究了那些在性别歧视与虐待问题出现时即刻应对的组织者，以及活动家们对转变性正义的实践探索。通过剖析活动家如何直面问题、弥合裂痕及女性主义应对策略，本研究为社会运动探索、替代性正义模式及性别化人际动态研究提供了新知。

[image]

初识"问责制"

2007年，我作为"要食物不要炸弹（Food Not Bombs, FNB）"分支机构的主要组织者，首次参与布鲁克林的活动家社群。该组织秉持纯素主义、DIY精神，与无政府主义思想相契合，收集原本会被浪费的食物进行再分配，且无需获得市政许可或授权。在为组织寻找厨房场地时，我发现了一个无政府主义社区空间，众多其他活动团体都在此聚会。FNB成员也逐渐开始活跃于使用该空间的其他团体，例如免费自行车维修工坊和给囚犯写信项目。其中几位成员更参与了空间的日常运营与维护工作。

这个社区空间成为我们进入更广泛的无政府主义与激进左翼活动家网络的入口。联系源于相似的政治诉求、共享的资源以及参与者间的社交关系。友谊、恋爱和/或性关系构成的社交纽带，塑造着团体形

态、及其在更大行动者网络中的定位。除日常工作和直接行动外，行动者们常举办音乐募捐活动为事业筹款，也共同参加非行动者的聚会。该社区秉持"性积极"理念，支持追求愉悦的态度，并倡导反羞耻话语。

参与这个自我认同的社群约一年后，一位空间里的朋友与前伴侣爆发了广为人知的矛盾。她告诉我正与一个名为"支持纽约"的团体筹备问责程序。一位共同朋友自愿担任调解人，她征询我对该人的评价。虽不了解具体流程，我仍陈述了个人见解并表示愿意提供支持。

我了解到所谓"问责程序"是组织者实践转变性正义与修复式正义的模式。不同于国家司法体系，问责程序聚焦于"幸存者"的需求（该术语将在后文详述），并致力于施害者的自我转变。在行动主义领域，识别虐待行为尤为困难 —— 因其表现形式多样，且往往需要承认那些被视为政治上正直的人实施的虐待。在问责程序中，施害者需同时接受幸存者及整个社区的追责。具体流程因情境而异且具有临时性。尽管女性、男性及非二元者都可能成为幸存者或施害者，但压倒性的模式是男性身份者对女性身份者、非二元及跨性别者的虐待。

当我决定启动问责程序时，我被介绍到了一个此前未知的社会运动领域。我加入了"支持纽约"组织，该团体运用转变性与修复式正义模式处理活动家亚文化中的性侵与虐待问题。我发现有几位朋友既是正在进行的问责程序中的幸存者，也是调解人。我们阅读、撰写并复制关于虐待与问责程序的小册子，就活动领域应对虐待的策略发表演讲，并在活动场所及活动中实施并执行安全空间政策。

围绕虐待与性别的问题无处不在，已成为活动家圈子中的争议焦点。处理此类问题的团体围绕"DIY正义"建立了洲际的和国际的合作网络，共同追踪那些拒绝承担责任的已知施暴者。关于虐待问题的热门杂志《革命始于家庭：直面活动家社群内的亲密暴力》于2011年由AK出版社出版成书。“支持纽约”组织的成员在2010年无政府主义书展及2011年占领华尔街运动中，推动制定了更完善的安全空间政策。

然而，团结至上的理念可能会掩盖特权和不平等的议题。"分裂的威胁常被用作达成一种勉强的且不愉快的团结的手段"（McRobbie 1997: 174）。部分活动家认为，根植于性别与性取向的问题优先级“较低”，或“依赖身份政治”，因而会分裂整个运动（Horn 2013）。围绕

此类意识形态危机制定战术和推进工作，往往是沿着性别界限展开的。

本研究聚焦行动主义内部的这些关系。我考察了当代左翼社会运动如何在社会正义的文化实验中回应女性、非二元者及跨性别者的需求。具体而言，研究探讨活动家为何在激进社会运动中建立"问责制"以处理问题，以及这些机制是否有效。借助皮埃尔·布迪厄的核心概念，本文阐释了应对人际暴力的DIY体制如何形成。我认为这些发展并非源于问题的激增，而是源于活动家围绕"社群"理念组织活动、适应预示性政治、定义和理解虐待行为方式的转变。我希望这项研究能为社会运动、亚文化研究和替代性司法模式的探索领域带来启发，并为持续应对这些问题的活动家群体提供参考。

[image]

方法论

尽管激进左翼亚文化中围绕性别与人际动力的讨论日益丰富，但其盛行程度并未体现在社会学研究中。值得关注的是女性、非二元性别者及跨性别者如何体验这些社会运动，以及他们通过哪些实践应对问题。

更具体而言，本文将探讨激进主义理想如何可能滋生性别歧视；激进派活动家为何开发正义设计来解决这些问题；以及，这对参与者的长期留存会产生哪些后果。

为探究上述问题，本文访谈了12位曾以幸存者、施暴者/加害者、流程协调员、调解团队成员或普通支持者身份参与问责流程的活动家。访谈内容涵盖其投身活动前在亚文化中的经历、问责流程本身、及其对流程有效性的评价。其中四位受访者为我个人熟识，其余受访者由已受访者推荐、或与问责制相关团体及文献存在关联。该样本虽未必能代表参与问责流程的所有未知群体，却能深入剖析其参与模式。所有访谈均录音存档，以确保记录中完整保留受访者的语言表达与情感状态，避免转述过程中的信息流失。

此外，我从左翼社会运动内部流传的小册子中收集补充资料。小册子

是亚文化产物，属于类似宣传册或手册的DIY出版形式，由个人、集体或合作团队撰写。其名称源于"杂志"，传统上通过个人或"分发集体"（distros）在活动相关场合或通过邮购进行复印传播。小册子涉及广泛议题，行文风格通常非正式、个人化且私密，类似日记体。激进运动中的性别歧视理论探讨、虐待性互动与关系的个人经历、转变性正义实践指南等，均已成为小册子的热门主题。

篇章组织形式

在后续章节中，我将探讨活动家如何应对性别歧视、如何创造正义形式，以及如何体验在激进左翼行动中的团结。参与者被赋权去建立亲密团队、组织活动、创作物品与艺术品。活动和策略受制于时间、地点、情境、可用资源及行动者意愿。反权威理念与现有资源及文化语境的结合，使行动强调**DIY**方法、愉悦感，且形式常具非正统性。

社会运动领域的行动者围绕文化实践与意义展开角力。在持续变迁的条件下，异质群体间的团结协作是催生社会变革的必要条件。对社会正义的共同诉求奠定了集体主张与行动框架的基础（Polletta and Jasper 2011: 285）。这种团结是参与者共同理解并分享的情感纽带。活动家们洞察不平等的模式，并将信念转化为实践行动。只要是以团结为目标，激进左翼活动家就绝不能容忍不公正，被边缘的群体亦不可继续被边缘化。

第一章回顾亚文化与社会运动的既有研究，以构建本研究的理论框架。首先将研究对象定位为"激进左翼亚文化"，需解析亚文化与政治的定义以理解其相互作用的关系，并考察亚文化内部文化形态及参与者间的关系。继而将研究对象视为"激进左翼社会运动"。社会运动文化植根于预示性政治，这种政治形态塑造了活动家对团结的认知及彼此间的互动关系。我梳理了布迪厄提出的并在资源动员理论中得到呼应的核心概念，这些概念有助于弥合传统学科间分歧，厘清社会运动团体内部的文化维度。综述结尾部分，我将考察部分学者和活动家提出的构建更公平正义社会运动的新模式方案。

第二章将阐述研究方法论。本研究采用历史文献考证、12位活动家的访谈及逾百份独立刊物的分析，并结合自身经历进行自我民族志阐释。这种多元方法论将深化对激进左翼亚文化中问责机制与转型正义

实践的广度与深度的理解。

在第三章中，我将把活动家当前面临的问题置于历史脉络中加以阐释。在1960年代末至1970年代初的新左派社会运动领域，同样存在诸多围绕性别歧视与虐待行为的类似问题。具体而言，我将梳理学生非暴力协调委员会（SNCC）、黑豹党以及民主社会学生会/地下气象员组织（SDS/WUO）等社会运动组织的浓缩历史。我关注活动家是否承认这些问题、如何协商解决，以及这些经验如何为DIY式行动主义的试错过程提供有益启示。同时将评估此类实践对运动产生的长期影响。

基于识别出的核心议题，我将分析划分为两章。

第四章分析左翼价值观与实践如何塑造跨越随意友谊、替代性另类家庭、性伴侣及恋爱关系的人际纽带。运动场域的社会文化环境催生出独特的生活方式。尽管存在反思性，活动家们仍不断挣扎于权力动态并屡屡重蹈覆辙。性别歧视以特定文化形态持续存在。

本节将考察组织运作中的差异，包括领导模式、会议机制及分工体系。随后聚焦性关系领域，探讨亚文化对同意原则日益强化的关注，以及运用文化与社会资本获取性伴侣的现象。最后将阐述源于1960-70年代运动的安全文化如何植根于前述资本形式，如何助长了性别歧视，并如何塑造运动内部问题讨论的优先级排序。

第五章延续分析框架，聚焦运动内部转变性正义模型的实践应用。组织者在左翼亚文化中推行新型的社区安全与正义机制，以对抗性别歧视、种族主义、恐同症及其他偏见。"安全空间"政策和以幸存者为中心的转变型正义及修复性正义实践，正揭示出诸多亟待解决的问题。我探讨了组织路径的构建与必要工作的完成、活动家如何共享信息、对虐待行为及关系动态认知的演变，以及围绕情感支持形成的社交纽带发展。

最后，第六章探讨转变性正义的实践成效。该领域的争议集中于实践与意识形态的兼容性，以及文化与社会资本的持久影响。并非所有被指控造成伤害的活动家都愿意接受问责程序，应对策略也各不相同。参与程序的活动家是否视其为“成功”，取决于他们对自身在运动中角

色的认知。相关活动家可能继续参与运动、转向不同领域，或彻底退出。这些程序的结果既关乎预示性政治的考量，也影响社会运动的延续性与持久性。

[image]

第一章 场景铺陈：激进左翼亚文化

我将研究对象定义为激进左翼亚文化，尽管这并非多数活动家的自我认同方式。参与者刻意将自身标榜为"社群"，而非采用"亚文化"或"反文化"等群体术语。

- "社群"一词暗示着超越享乐追求或风格特质的实体与意识形态稳定性。这个词汇承载着多重隐喻，如同咒语般在行动主义词典中被反复宣示和暗示。它成为泛指一切的万能标签，是我们用来指代共同体的代名词，借此传递与盟友间的战友情谊与亲密感。

- 偶尔会出现"酷儿"或"无政府主义者"等描述性词语置于"社群"之前，但多数情况下参与者既不具体说明也不定义这个词。

- 被纳入该范畴者需自行推敲成员资格的内涵，由此形成流动包容的特性。它既反映环境的语境变迁，也承载个体的生命历程。

为避免歧义，我将研究对象定义为亚文化。尽管本文中我用“社群”指代这种文化群体，但其与更精确的亚文化概念具有互换性。

第二个描述性限定词我选择使用"激进"。部分社会学家曾使用"无政府主义者"或"新无政府主义者"描述类似社群，尽管这些团体和个人在运作中“并没有明确采取无政府主义标签”（Gordon 2007: 32; Robinson 2008, 2009; Shepard and Hayduk 2002）。这些学者认为，活动家的意图本质上是无政府主义的，只是暴力行动的负面联想及残酷镇压

促使他们回避这一身份标识（Gordon 2007; Robinson 2008）。不过研究者若笼统使用无政府主义标签会淡化亲密团队的形成、联合、争执、瓦解的历史进程，以及激进行动的多样性。"无政府主义者"逐渐沦为子类别，导致个人可能同时参与标榜无政府主义的团体和回避该标签的团体。例如将整个社群统称为无政府主义者，当活动家表示"目睹无政府主义圈的动荡后，我将注意力转向女性主义圈"时，其区分的意义便被抹杀，研究者的分析也随之偏僻（Exposito 2011）。

活动家们使用"激进"一词时旨在表明自己与以往社会运动的区别，即采取"更根本的革命立场"（Eisenstein 1984: 127）。他们致力于解决与成员文化体验相关的问题，并认识到反全球化、反战、反新自由主义、生态主义、反资本主义、反种族主义与女权主义之间的交叉关联。活动家们共享一套明确的激进议程，并基于对抗问题根源 —— 即现行权力结构的认知与行动，构建集体认同。作为无政府主义、反资本主义、反种族主义、女权主义、酷儿运动等激进政治团体的融合体，其意识形态虽未必完全一致，却存在内在延续性。"激进主义"一词避免了"无政府主义"的负面联想，在自我认同时常与"无政府主义"互换使用。

在本研究中，我将聚焦于社区的内部文化。在我们的环境中，如果将行动主义仅局限于直接行动范畴，就只会割裂活动家们多元化的努力以及公民行动所蕴含的多重意义。成员们通过共享差异与文化实践参与其中，从而确证其归属感。"仅靠示威标语是远远不够的"，更需关注参与者的经历、思想与行为（Zimmerman 1993: 52）。围绕预示性政治 —— 即在日常活动与互动中实践替代性方法 —— 已形成独特的行动主义亚文化。

作为激进左翼亚文化

亚文化作为颠覆性存在

我所研究的文化最适宜归类为"行动主义亚文化"。"亚文化"的历史演进使其与政治立场产生了交融。英国伯明翰大学当代文化研究中心（CCCS）将二战后兴起的青年文化视为"亚文化"，这一术语揭示了阶级分化及其引发的颠覆性力量。工人阶级亚文化群体通过培育独特风

格与休闲实践，象征性地表达出"与主流文化及意识形态实践的对立关系"（Willis 1977: xiii）。

CCCS理论家运用符号学"解读"这些表演行为 —— 它们通过商品拼贴实现，其中"文本"被碎片化，旧有意义在重组过程中被颠覆或替换为新意。亚文化理论揭示这些商品被主流文化赋予了看似自然的"意义、联想与社会内涵"，而亚文化群体通过改造这些符号以进行抵抗（Clarke et al. 1976, p. 55）。朋克亚文化的嘶吼歌词、泰迪男孩的"绅士"着装、摩德族的小型摩托车，皆传递着对所处环境的批判。由于此类研究多聚焦男性主导的亚文化，安吉拉·麦克罗比和珍妮·加伯于1976年指出："女性在整个文化研究领域的缺席 ... 令人震惊，亟待解释"。

新近理论家重新审视了CCCS的研究及其符号学遗产，批评其将"亚文化"标签局限于工人阶级，并假设阶级文化在阶级界限上是同源且明确区分的（Muggleton 2000, Thornton 1996）。更近期的研究，如戴维·马格尔顿的《亚文化内部》等，发现亚文化群体往往不愿认同特定政治意识形态或团体，认为这实另一种形式的"强加权威、顺从与统一"（2000:150）。米歇尔·马费索利等理论家重新定义亚文化为"新部落"，其核心在于生活方式，"注重表象与形式"，不设明确的包容与排斥界限，而强调重叠的归属关系（1996:98）。尽管可能存在抵抗氛围，但这些理论家认为其往往是对主流或顺从文化的模糊抗拒，而非针对更大权威体系或权力的反抗。

因此我采用"行动者"这一指称来界定研究对象。激进左翼亚文化确实符合CCCS的定义标准。尽管并非所有行动者都来自工人阶级，但多数成员具有此背景，且该亚文化植根于工人阶级价值观。符号与意义的建构与改造在文化领域表达了这种对抗，形成"反霸权的个体与集体抵抗形式"（Brotherton 2008: 55）。它在意识形态、话语和行动层面明确挑战现行秩序。更具体而言，它符合霍尔对革命性亚文化的标准 —— 即"提供体现替代性结构的行动形式"（2007:6），同时也满足霍兰德与艾因韦纳提出的抵抗标准 —— 包含行动、对抗、认同与意图（2004）。植根于社会正义的文化实践，有力推动了横向组织与自主自治的发展。

行动者亚文化

行动者亚文化之所以独特，在于它们共享休闲活动与审美风格的同时怀有明确的政治诉求。这并非否认休闲与风格在行动者亚文化中的重要性，但集体认同的根基是在于对抗更大权力结构的认知与行动。该亚文化的美学特征浸透着政治符号，如黑色连帽衫、自行车、日程本和可重复使用的水瓶。不同于大多数当代文化研究中亚文化的样本特征，该亚文化参与者普遍年龄稍长（二十岁出头至二十五岁左右），正处于围绕政治意识形态定义自我、构建人生的阶段。

如同马费索利所论的新部落，我研究的亚文化融合了多重交叠的文化归属（Muggleton and Weinzierl 2003）。一些学者质疑以政治为中心和以享乐为中心的亚文化之间的区分是虚假的建构。"抗议狂欢"与"无政府主义集市"的兴起，正是"致力于享乐与政治"的矛盾元素融合的典型例证（St. John 1997:65）。斯图尔特·霍尔虽区分了这两类群体，却假设亚文化中的两个"极端"实则相互交织。个人主义表达"强调个人...文化...审美"，"发展...革命风格"并"提供...言语"；而行动主义则"强调政治、社会、集体...组织承诺"，"提供社会塑造力、组织力与推动力"（Hall 2007:165）。

激进社群的独特文化折射出政治理念与宏观文化实践的互动。流行"潮人"青年文化正与这些激进左翼亚文化相呼应。潮人美学与生活方式的中心位于都市区域，更具体而言是布鲁克林的威廉斯堡与布什维克街区。潮人的定义具有主观性，并且符合这一标准的人通常都不会如此自我标榜 —— 换言之，所有人都是潮人，却无人自认潮人。社区社交活动吸引着部分平日不参与社会运动的人群，例如曾每年举办的"反情人节暴动女孩翻唱乐队演出"。活动家们也常参与非抗争性质的聚会，例如仓库乐队和麦基本阁楼的地下演出。这种重叠现象在《纽约新闻》题为《认识助人青年》的文章中得到了最佳诠释 —— 非营利组织"邻里求好发展联盟"成员艾米丽·加拉格尔坦言："如果没有啤酒相伴，我们在NAG很难找到真心愿意做志愿服务的人"（Richards 2010）。其中部分活动本身属于激进社群或与其存在关联。这些轻松愉悦的行动主义形式，为人们提供了超越常规酒吧和俱乐部的社交空间。

亚文化中的文化内核

尽管服饰与发型在亚文化中占据重要地位，激进主义群体却没有如此精确的时尚规范。如前所述，黑色连帽衫是该亚文化中所有性别成员

的标配，这很大程度上源于其在黑群示威活动中的使用。黑群行动是一种直接行动形式：参与者身着全黑服装，遮掩面部与头部，集体游行。全黑装束与面部遮蔽使活动人士得以在执法部门面前保持匿名，同时彰显群体规模。

另一常见物品是弹弓或"正义种子"计划本，这两种由活动家团体制作的工具，能帮助活动人士同步日程并追踪行动和事件。普遍使用的自行车和水壶彰显了环保理念及对浪费与消费的抵制。除此之外，着装通常反映当前朋克与潮人时尚，辅以常规牛仔裤和T恤。几乎所有激进活动家都至少拥有一个纹身，但位置、尺寸和内容各异。少数活动家是专业纹身师，常被同行寻求合作。另有少数亲活动家纹身店公开服务纯素食者，或为各类公益事业提供合作支持。但纹身终究是"一种完全可接受的另类时尚形式"，其流行绝非仅限于布鲁克林的活动家亚文化圈（Pitts 12: 2003）。

尽管该亚文化以政治理念为根基，其行动模式却颇为复杂。所谓"深层结构"，即"支撑决策与行动的、被视为理所当然的价值观、思维方式及工作模式集合"（Rao and Kellehon 2005）。这些无形规则与人际关系在活动家群体中自然形成。由于"思维地平线"具有隐形性，激进左翼活动家们在抗争某些权力动态与预设观念的同时，却也在无意间复制着它们。

正如妮娅·金在其杂志《最初的七英寸更美好》所言：

> "我们以最直白的方式标榜'酷儿'，以最白人化的姿态宣称'反种族主义'。

众口一词自诩女权主义者，为何性侵事件仍在圈内反复发生？我们为移民权利奔走却从未接触移民，举办同意权工作坊却不知如何追究每日相见的施暴者。" 正如对其他政治亚文化的研究所揭示的，活动家们"总强调男女在组织中享有平等地位，性别议题服从于群体团结 ... 然而在诸多问题上，内部存在深刻裂痕"（Brotherton and Barrios 2004: 192）。

[image]

内部等级结构

尽管许多研究探讨了主流文化与亚文化之间的关系，但鲜少有人考察亚文化内部的社会文化力量。在各种亚文化的定义中，一个普遍特征是其与主流文化的区别性。成员们感受到这种区别性，并由此产生归属感。当代行动主义亚文化虽曾因围绕本质主义身份组织而遭到批判，但现已意识到了反本质主义与身份政治的重要性。组织者们洞察到种族、阶级、性别及性取向方面的不平等模式，持续开展关于反思性、特权意识及"团结"呼吁的对话。

自文化研究领域萌芽之初，女性主义理论家便批判了对女性亚文化实践者隐性排斥的现象。安吉拉·麦克罗比在早期亚文化组织研究中发现，性别是亚文化内部的"核心组织原则"（2000:14）。少女文化、她们在亚文化中的成员身份、所扮演的角色以及自我定义方式均需深入探究（2000:14）。麦克罗比承认这种缺失部分源于研究者被认定的性别身份。由于"女孩封闭而多疑的世界"（2000:4），接触女性及获得其沟通意愿往往困难重重。民族志学者与女性参与者之间的互动动态，会因研究者性别差异及进入更私密的研究场域而发生变化。

多位女性主义学者发现青年亚文化中存在男性特权的社会等级（Reddington 1997, Leblanc 1999）。多琳·皮亚诺观察到年轻男性朋克会保护女性朋克免受外人侵害，却在朋克文化内部对她们进行骚扰与物化（2003）。女性朋克的角色定位在于"行动"（制作杂志、组建乐队、阅读杂志、组织会议）而非"被观赏"（作为景观被看待）（2003: 254）。诺玛·门多萨-丹顿研究的帮派女性成员奉行"先笑后哭"的准则，以强悍外表掩饰真实情感。帮派外的群体则批判女帮派成员的美学形象，当她们不符合文化观念定义的“女性气质”时，便被贴上女同性恋标签（2008）。南希·麦克唐纳发现女性涂鸦艺术家必须更频繁地在更困难的场所"露面（留下作品）"，以证明自己并非"怯懦娇弱的小东西"（2001: 130）。女性特质遭贬抑，而被贬抑者又被女性化。总体而言，“男性……努力证明自己是‘男人’，而女性……必须努力证明自己不是‘女人’”（麦克唐纳 2001: 130）。

尽管激进亚文化明确反对社会不平等并倡导女权主义，其独特的文化资本体系内部仍存在类似的性别分工。与其他行动主义群体及社会运动相似，性和/或浪漫关系在此广泛存在，且影响深远（Shepard 2005, Goodwin 1997）。集体沸腾状态、亲密关系网络与性自主权的结合，构成了浪漫人际关系的理想温床。摆脱传统生活方式的束缚，也使得性别与性取向的定义和表达更为流动。本·谢泼德在《将欢

愉作为社区组织策略》中指出，游行活动既是结识魅力人士的场所，也是"寻觅"性伴侣的空间（439–440页：2005）。在激进派社区文化中，持续不断的深夜住宅派对、乐队演出和舞会，进一步拓展了这些关系的可能。而当社群纽带断裂时，往往意味着参与社会运动的终结。

[image]

作为激进左翼社会运动

预示性政治

个人实践与政治意图的融合，为激进左翼行动者亚文化群体提供了多种议题和方法来推动社会变革。参与实践蕴含着预示性政治（Gamson 1991），即"对新型文化模式的实验与实践"（Melucci 1989: 60）。然而政治诠释并非同质或固定，其中存在麦卡丹所谓的"认知解放"的过程，即对结构性不平等"状况的合法性与可变性"的集体认知（McAdam 1986: 35）。

该过程并非真空发生，而是在更广泛的文化规范与行为中平行发展，"孕育于革命前社会的子宫之中"（Hall 2007: 163）。

[image]

将意识形态主张应用于物质现实的尝试，正是通过试错和协商形成的预示性政治。其成果具有碎片化特征，并因参与者、情境及政治伦理而呈现差异化。

参加集会、游行示威、撰写博客、筹办募捐活动、在公共场合摆摊——这些行动都与活动家的日常工作、学业和家庭责任交织在一起。参与者必须将社会正义信念与现实环境相协调，从而形成多元化的生活方式。

在预示性政治的实践中，社群将重心转向能动性与重大变革的可能。抗议行动与休闲活动的界限逐渐模糊。激进左翼亚文化鼓励创造力和

艺术探索，参与者被赋权组建亲密团队、策划活动、开创新项目。活动家们"以个人生活预示其战略目标"（Williams 2016: 74）。反权威理念与现有资源及文化语境的结合，使行动强调DIY方法、追求愉悦，且形式常具非正统性。

激进社会运动的预示性政治具有实验性，其摆脱社会不公根源（即国家）的自主需求，要求集体开发替代性模式（Scott 2014: xxi）。

这种实验发生在不断变化的背景下。

[image]

新社会运动文献指出，社会运动并非经验对象，而是互动过程。与其将社会运动视为具有明确凝聚点、议程和方法的独立实体，不如将其理解为持续进行的理念和意义的协商。

个体之间通过协作定义目标、行动和约束条件，同时相互沟通以"组织"集体行动。

这种"构建认知框架"的过程塑造了活动家的参与方式、"关系网络 ... 以及 ... 情感投入"（Melucci 1989: 35）。

活动家们试图基于承认等级制度和不平等的文化图式，实践另类生活方式。种族、阶级、性别与性取向等议题，始终在反思性、特权意识和团结呼吁的持续对话中展开。活动家们注重去等级化的权力分配、共识决策与公平分工（Holland, Fox, Daro 2008, McDonald 2002, Bevington 2008）。实践中的这种预示性政治，既承认社会分层的存在，又通过非等级结构实施反制。群体内部的运作模式体现着共同的社会正义政治。为维持权力平衡，部分参与者将视线转向内部。乌里·戈登在研究无政府主义亚文化时指出，人们承认"支配模式在社区内部和/或社区间重新浮现，即便在某个时间点它们已被有意识地克服"（2007:45）。目标并非追求统一，对交叉性的认知也不同于利益或方法的统一。更精确地说，目标是在不断变化的异质性环境中相互支持，且不存在等级制度和施舍心态。那句耳熟能详的口号"另一个世界是可能的"，正体现了对这种预示性政治及社会正义组织实践的坚定信念。

打破等级制度以组织并挑战现有权力结构，对社区的集体团结至关重要。团体采用去等级化？或水平式结构，成员间不存在权威或等级差异（Fitzgerald and Rogers 2000）。每位成员必须明确表态是否赞同、反对或弃权。群体尊重每位成员的意见并需达成共识。共识机制为表达观点提供了明确渠道，有效防止话语权被垄断。

[image]

尽管这类群体理论上脱离等级制运作，领导者仍会自然涌现（Freeman 1972, Sahasranaman 2013）。

如果不能有意识地平衡权力，社会特权者往往继续在激进团体中延续其支配地位。

应对这种不平等的策略之一是将文化植根于DIY（自己动手）理念。**DIY**本质上注重自主权和可及性，个人或团体可自主定义项目内容、实施时间、地点及方式。这种模式赋予更多灵活性与即时性。组织者在协作中发展并共享优势与技能，为艺术创造开辟新的可能性。

[image]

DIY伦理的核心在于：任何人都能（且应当）在不受金钱或技术限制的情况下表达自我。

DIY强调自主赋权与自力更生，而非依赖他人。

由于个体能自主组建团体，既有的社交网络可以促进团体发展并塑造成员构成。

DIY精神往往促使人们在既有友谊网络中组织行动（Freeman 2009）。但这种模式并非没有代价 —— 活动家们为此付出大量的时间、精力、甚至自掏腰包。

准入与网络

招募对亚文化有着深远的影响。人们在决定是否参与行动主义时，并非出于工具性推理（Melucci 1996）。虽然意识形态上的认同看似是最明显的参与理由，但仅有不满和被剥夺感并不足以解释个体参与社会运动的行为（Melucci 1989）。

除了共同的意识形态之外，人们的社交关系网络、文化背景和个人经历，都会影响一个人参与社会活动的可能性（Ibrahim 2011, Blee 1991, Passy and Giugni 2001, Melucci 1996）。虽然人们可能会认为那些没有既定目标的、时间精力都比较充裕的人"更容易参与"，但"个人经历的可及性"与社会运动参与之间的关系远比这复杂得多（McAdam 1986: 70）。按照这种逻辑，我们很容易解释学生积极参与社区活动的原因。然而，仅凭个人经历的可及性不足以解释参与的原因。那些更空闲、有时间和能力的人并不一定会参与行动和活动；与预期相反，那些已经在社会和政治上积极参与的人则更有可能投身社会运动（Verba et al. 1995, Munson 2010）。

那些进入并参与激进社群的人，往往正处于人生的过渡阶段。过渡阶段是指日常生活和人际关系网络发生变化，人们"更容易接受新思想和新的世界观"（Munson 774: 2010, Robinson 2008）。人际关系网络的变化会带来新的关系发展，并使他们有机会接触新的思想和文化（Taylor 2000: 222）。这些关系和友谊是社群招募成员的重要资源（Taylor 1989, Snow, Zurcher, and Ekland-Olson 1980）。参与者常常通过社交关系被吸引到社群中。寻求工作或教育的年轻人经常涌入城市中心，导致大量潜在的社群成员正处于人生的过渡阶段（Roberts 2013）。社交关系决定了谁能加入社群，以及谁不会加入，进而影响社群的性别、年龄和种族构成。

[image]

延伸：https://iyouport.substack.com/p/34b?utm_source=publication-search

延伸：https://iyouport.substack.com/p/4d9?utm_source=publication-search

返回 - 纸条：[image]如何选战友

亚文化内部结构是由志趣相投的群体和个人组成的网络（Melucci 1996，Jasper 1997）。该网络结构紧密，群体和个人之间存在重叠。志趣相投的群体是非正式的、非永久性的组织形式，专注于特定议题。例如，“For the Birds”是一个关注女性创意活动的女权主义团体；“POC Zine Project”是一个致力于推广和发行有色人种创作的独立杂志的团体；“Ghost Bikes”是一个为骑行者发声并为在城市中遇难的骑行者建造纪念碑的团体。志趣相投的群体会随着时间的推移而形成、重组和解散。群体的流动性导致这些群体间网络关系较为松散或短暂。本地志趣相投群体的兴衰会改变社区网络的结构。

亲密团队的成员人数较少，它们建立在参与者彼此间的社会关系之上，或促进了这些关系的发展（Pickerill 和 Chatterton，2006：740）。由于个人有能力且有权创建自己的团体，现有的社交网络可以促进群体发展并塑造群体成员构成。这种DIY精神往往促使人们在自己的友谊网络内进行组织（Freeman，2009）。新的群体内部关系会改变社交网络，而友谊的破裂则可能导致团队的解体。

[image]

团结

女权主义的常用表达“个人即政治”与预示性政治具有相似性，尽管前者还包含情感和亲密的内涵。卡罗尔·哈尼什于1969年2月发表了一篇同名文章。这篇文章是对当时激进运动的回应，这些运动将妇女团体“讨论自身所受压迫的行为斥为‘自我凝视’和‘个人疗愈’—— 当然更谈不上‘政治’”（Hanisch，2006）。哈尼什认为，个人经历在政治行动主义中应被视为合法的且相关的。阿尔贝托·梅卢奇在其著作《当下的游牧者》中指出，社会运动的内部张力正日益集中于人际关系和生活方式。冲突既“日益个人化，围绕着个人发起行动以及掌控空间、时间和人际关系的能力展开”，也“旨在‘建构意义’”（梅卢奇，1989，71）。

社会运动的维系需要构建替代性的文化框架，以及个人对这些框架的投入。参与者是否感受到团结，以及运动文化是否能够适应他们的需求，都可能决定运动的可持续性（Gecas 2000，Collins 2001）。

梅卢奇将团结定义为群体成员之间人际互动的结果；“行动者承认他

人并被他人承认属于同一社会单元的能力”（1996：23）。行动者是否拥有共同的信仰或意识形态并非必要条件，但团结的建立和维系比工具性目标更为关键（Melucci 1996：103）。我认为团结是对同伴关系的认可，这种认可既植根于对社会正义的共同信念，又体现在与同伴行动者的互动中。构建行动者“社群”是一个过程，一项持续不断的努力（Scott 1992）。

团结意味着一定程度的互惠关怀、责任和相互依存。归属感塑造了社群，而社群也塑造了谁觉得自己属于这里。

杰奎琳·肯内利（Jacqueline Kennelly）在一项针对加拿大年轻城市活动家的研究中发现，参与者的种族和阶级极大地影响了他们的成员感和归属感。不言而喻的知识决定了权力，进而影响了参与者的成员感和归属感。

许多亚文化规范源于“中产阶级青年认同工人阶级身份，或模仿颓废摇滚”（304）。尽管这些亚文化群体展现出较低的社会经济地位，但他们将行动主义定义为一种慈善形式，即“一些人为他人所做的事情”（299），这体现了他们的特权地位。下层阶级和有色人种“体验到一种‘格格不入’的感觉”（301）。肯纳利发现，这种融合的缺失导致这些人退出了社会运动。同样，玛丽亚·扎卡里亚森在对斯堪的纳维亚全球正义活动家的研究中发现，年轻的男性参与者认为他们的存在是为了“为他人而战：受压迫的妇女，世界上的穷人”（2009：36）。

关系与性

多项研究表明，人们加入社会运动更容易“用人脉关系来解释，而非用他们的意愿或信仰来解释”（Kitts 1999）。既有的和正在发展的社会关系是团结建立和替代性文化蓝图得以成功的重要因素（Passy和Giugni 2001，Gamson 1991，McAdam 1982）。

[image]

参与者 融入情感关系网络的程度 会影响他们参与社会运动的程度。

友谊和性关系，例如“集体”和“团结”等概念，极大地促进了归属感的形成。尽管社会正义问题很重要，但人际关系对亲密团队的发展、成员构成和群体间的联系，有着显著的影响。

通过参与而建立的关系塑造并维系着激进社群。行动者之间建立的联系构成了人际关系网络，既促进了团结，也阻碍了团结。杰夫·古德温在研究菲律宾虎克起义时发现，行动者之间的情感关系创造了一种力比多经济，在这种经济中，人际互动的愉悦感取决于情感联结和相互的爱慕，从而形成了一种“情感纽带的结构和经济”（53:1997）。虽然“力比多”一词通常指性关系，但古德温对这一术语的使用涵盖了其他由“爱”的感觉所定义的各种关系形式（54:1997）。因此，力比多纽带涵盖了性关系、家庭关系、友谊以及对人类的爱。

[image]

返回：

返回：

返回：

在“团结互助”群体中，力比多纽带的运作方向有两个（Goodwin 55: 1997）。

- 第一个方向是与群体和/或事业的关系。

就我研究的人群而言，力比多纽带存在于作为运作实体或另类家庭的激进“社群”之中（Halberstam 2006）。这种纽带将群体和/或事业与社会其他部分区分开来。参与者的道德意识融入了集体情感，并阐明了价值和美德体系。

戈登在其对新无政府主义团体的研究中指出，参与者的凝聚力“超越了个人关系层面”，创造了一种“部落式团结”，在这种团结中，同伴行动者“被视为自己大家庭或部落的成员”（Gordon 2007: 33）。与传统家庭不同，行动主义者可能会通过一起纹身、志愿参与行动主义以

外的项目、在肢体冲突中声援彼此，或者在夜幕降临后一起骑车回家等方式来表达成员身份。

除了直接的人际关系之外，他们对整个社区的义务或责任可能包括护送醉酒的陌生人安全回家，或者为临时来访的朋友的朋友提供住宿。

- 第二种方向就是群体内部的性欲纽带。

作为一种经济体系，反复的互动和相互情感的建立会形成人际关系。对事业和意识形态的共同认同会产生信任和忠诚；“我们信任与我们意见一致的人，也认同我们信任的人”（Jasper 1997: 112）。

建立这些关系的稳定性和难易程度极大地影响着参与者的投入程度（Taylor 1989）。因此，参与者人际情感的强度和互惠性加强了他们与群体的力比多纽带。

参与、加入和组织社区活动都存在情欲动机。在对女权运动的研究中，维尔塔·泰勒发现与女性结伴可以“促进女权主义工作，因为这些女性的个人生活与她们的政治承诺非常契合”（Taylor 770: 1989）。

性关系促成行动主义项目的情况并不少见。组织者将一夫一妻制、多角恋、S&M、以及其他各种性行为形式与政治联系起来，并付诸实践（Portwood-Stacer 2010）。虽然这些联系有助于甚至可能加速人们的参与，但与外界人士的关系也可能阻碍他们参与社会活动。

[image]

延伸：https://iyouport.substack.com/p/efb?utm_source=publication-search

延伸：https://iyouport.substack.com/p/270?utm_source=publication-search

[image]

权力、文化与实践

布迪厄的分析框架

亚文化的动态可以通过布迪厄的场域分析框架来考察。场域是结构化的空间，行动者在其中通过相对形式的资本来争夺权力。场域边界并非固定不变，而是与其他社会场域相互联系。场域中的行动者拥有共同的文化理解、场域规则以及对规则的感知（Bourdieu，1990：66）。

场域内个体的行为，包括其归属/参与某一特定场域的行为，都受其惯习的影响。个体的惯习是指其作为社会群体（即阶级）成员所具有的禀性。惯习"内化为一种第二天性"，并且"倾向于在场域规范内产生所有'合理的'、'常识性的"行为'"（Bourdieu，1990：56）。

[image]

惯习以一种看似自然的方式再生产社会分层，

因此它既受社会分层的影响，又塑造社会分层。

文化资本在文化中再生产社会分层。文化资本是指那些被文化赋予价值、嵌入文化之中并代代相传的知识，这些知识可以是客观存在的、具身的或制度化的。被赋予价值的事物往往与权力更大的人相关联，被认为是自然的或客观的现实，并且"是通过某种摆脱经济需求的方式获得的"（Bourdieu，1984：54）。当文化资本客观存在时，它"以文化产品（图片、书籍、词典、乐器、机器等）的形式存在"（Bourdieu，1986：243）。当文化资本具身化时，它"被视为内在本性最自然的表达"（Bourdieu，1984：192），并"转化为……一种惯习"（Bourdieu，1986：245）。

布迪厄还探讨了社会资本作为复制权力动态的一种手段。社会资本是"与拥有持久的……相互认识和认可的关系网络相关的实际或潜在资源的总和"（布迪厄，1986：248）。这些成员身份可以作为一种"凭证，使其持有者在各种意义上获得认可"，并允许各种形式的资

本和资源交换（布迪厄，1986：249）。这种资本不仅取决于关系本身，还取决于持有者调动其网络的能力。

布迪厄认为，惯习、资本和场域共同决定了实践的产生，其关系可以用以下等式表示：[(惯习)(资本)] ＋ 场域 ＝ 实践（Bourdieu，1984：101）。个体的惯习和资本形式，在场域和“游戏”规则的背景下，会形成实践，而实践反过来又会“决定”生活方式（Bourdieu，1984：171）。生活方式是实践和品味的集合，在看似独立的生活领域中形成一种同源性或“主题”。尽管品味似乎是一种个人决定，也是区分我们作为个体的一种方式，但布迪厄认为它是“标记同一惯习所有产物的特殊印记”（Bourdieu 1990：60），或者说是“系统地表达特定阶级生存条件的独特特征系统的来源，即一种独特的生活风格”（Bourdieu 1984：175）。

将布迪厄理论应用于亚文化和社会运动

就社会运动而言，布迪厄因将“惯习和假设”与“话语、理性和反思”对立起来，而受到批评（Crossley 2003: 48）。这与资源动员理论形成鲜明对比，后者强调此类集体行动中涉及的能动性和理性。尼克·克罗斯利认为，布迪厄对社会运动的考察往往局限于暂时性危机的视角，而非既定的社会场域和惯习的发展。惯习“汲取了一系列在历史和文化上不断变化的抗议‘技巧’，行动者从中学习：例如，请愿、游行、占领、挖掘隧道和制造炸弹”，以及“即兴发挥或 …… 行动者创造新技术以丰富现有技巧的潜力”（2003: 49）。

一些理论家将布迪厄的“场域”概念应用于集体行动和社会运动，称之为社会行动场域（SAFs）或“争论场域”（Crossley 2003，Fligstein和McAdam 2011）。这些场域拥有自身的“游戏规则”、惯习和资本形式，从而形成特定的行动实践。行动者的生活方式，包括他们的行动、工作、文化产品的使用以及社会生活，都由他们的政治立场和实践活动所定义。

布迪厄的文化资本概念已被修正，用于研究亚文化内部的文化实践。莎拉·桑顿在对英国锐舞者的研究中发现，亚文化群体在亚文化层面复制了既定的等级制度，并将“时髦”视为一种资本。“酷”取决于特定文化所看重的价值观和知识。“亚文化资本”源于“消息灵通”、穿着“得

体”的服装、拥有“合适的”发型、喜欢“合适的”音乐，以及在特定情境中恰当地展现肢体语言（1996）。这些被重视的习俗、审美和知识相应地体现了一个人的亚文化资本。另一方面，性别则更为重要。对于桑顿研究的锐舞者而言，阶级可能是一个因素，但它通常“被亚文化差异有意掩盖 …… 一种无阶级的幻想”（1996：12）。女性亚文化群体成员要么“承认亚文化等级制度并接受其低下的地位”，要么如果她们参与其中，她们会“拒绝和贬低女性化的主流”（1996：13）。相反，女性往往承认、维护，有时甚至采纳那些赋予男性和男性特质特权的社会等级制度。

在社会运动研究中，资源动员理论在探讨社会运动的创建和动员时，考虑了“文化资源”和“社会组织资源”这两个组成部分（Edwards and McCarthy 2007）。文化资源包括抗议策略、与新闻媒体沟通的方式、组织团体会议以及创作音乐、视频和出版物等文化产品。拥有这些资源的个人或团体可以被认为拥有文化资本或亚文化资本。社会组织资源是指能够促进招募和动员的社会网络和组织关系。这些资源可以直接与布迪厄所谓的社会资本概念进行比较。

在激进亚文化中，“消息灵通”意味着掌握最新最有价值的信息。熟悉诸如“zines”（独立杂志）、“infoshop”（信息商店）、“COINTELPRO”（反情报计划）、“CrimethInc.”（犯罪集团）等常用词汇和俚语，以及无政府主义、马克思主义和社会主义理论及领袖人物，都是文化资本的象征。此外，如果有人协助组织规模庞大的秘密行动，或者掌握一些鲜为人知的信息，活动家们会格外重视。作为活动家的声誉和社交网络关系可以巩固其地位。那些被认为足够重要或危险，以至于引起中央政府“关注”的活动家也备受推崇。

在某些情况下，懂得不谈论某些信息，即恪守安全文化，本身就是一种资本。

“安全文化”指的是社群内部对保密的需要。安全文化是激进活动文化中各个方面谨慎行事的简称。它规定了谁应该或不应该掌握敏感信息，以及何时何地可以讨论这些信息。具体原理见下面标注。

[image]

返回 - 自卫措施：[image]信息最小化原则

据此原则，活动人士可以做到尽量把违法的或被禁止的活动限制在有限的群体内。

对国家通过直接或间接监视进行镇压报复的恐惧，指导了这些政策。这些信息可能涉及过去发生的事情或未来将要发生的事情，也可能涉及某个具体的行动或人物。由于安全文化的存在，活动人士的秘密行动本质上具有排他性。

那些经常掌握独家信息或身居（非官方）领导职位的人往往是顺性别男性。在少数内部纠纷中，女性、非二元性别者和有色人种感到在“安全文化”的幌子下被噤声。当他们批评组织者没有让他们参与时，人们常常以“安全文化”作为笼统的回应，这让人质疑反对者对社会正义的承诺以及他们作为行动者的真实性。援引“安全文化”既可以诋毁对手，又可以维护自身的真实性，从而平息争论。正如阿金·桑顿笔下的锐舞者，吹嘘高风险活动会削弱亚文化资本。

社会运动中的社会公正文化

在对社会运动中的性别问题进行年度评估时，“桥梁计划”论证了“性别公正”运动的可能性。这类运动需要“自我批判……以及在人们努力重塑自身信仰体系和政治世界观的过程中给予的耐心和支持”（Horn 2013:66）。由此产生的社会运动：

- 确认解决性别不平等和父权权力是实现所有群体公正不可或缺的一部分，并将其明确列为行动的优先事项。

- 营造积极的环境，以进行内部反思，并就女性权利和性别公正采取行动。

- 为女性参与和领导运动实践的各个领域提供积极和正式的支持。

- 始终致力于解决基于性别的暴力问题，并对运动场所中的性骚

扰采取零容忍态度。

- 评估运动角色中的性别偏见，并按照性别公正的原则重新分配劳动力。

- 使所有人都能充分参与，同时顾及到照护工作和生育角色。

- 认识到活动人士所面临的反弹和外部反对的性别因素。

- 探讨与性别相关的规范和观念，同时考虑到特定语境下的性别认同、跨性别和双性认同，以及社会生活和行动主义中不断变化的性别理解。（Horn 2013：5）

尽管做出了种种尝试，但我研究的激进左翼社会运动在其预示性政治中并未达到这些标准。

许多女性、性别非二元人士和跨性别者在激进左翼亚文化中面临性别歧视和虐待。缺乏团结和支持导致他们改变参与方式或选择离开。正如一位独立杂志作者所言，年轻女性“最终主要被视为性对象，最终对男性主导的圈子感到失望，然后离开”（Said the Pot）。此前的学术文章和调查性新闻报道曾提及其中一些问题（Schneider 2013，Graeber 2009），但并未具体探讨这些问题，而是侧重于分析该运动所宣称的政治目标。

[image]

当社群和个人界限变得模糊不清时，行动者必须保持道德操守，

并对权力动态保持清醒的认识。

尽管《桥梁报告》并未对“深层结构”的动态进行深入研究，但它提出了社会运动发展“正式的问责方法和问责结构”（91）的问题。

[image]

亚文化必须在既有的相互问责和维护意识形态信念的途径与避免复制国家结构之间找到平衡。社会制度的重建需要考虑激进行动者的惯习性、资本形式、以及由此产生的生活方式。

我研究了当代左翼社会运动如何应对这些问题，希望以此阐明预示性政治的过程。具体而言，我的研究探讨了行动者为何要发展“问责制”来处理激进社会运动中的问题，以及这些机制是否有效。

[image]

第二章 方法论

尽管社会运动是社会学的常见研究课题，但人际互动问题，特别是性侵犯问题和转化性正义，在学术界却鲜有涉及。大多数社会运动研究都将其置于更广泛的社会背景及其政治目标中进行考察。这种研究的匮乏似乎与某些激进分子的观点不谋而合，他们认为情感和人际关系是“琐碎的问题”，存在于社会运动之外。然而，对于那些参与激进亚文化的人来说，性别议题和转变性正义问题是至关重要的。

我研究的激进左翼亚文化群体围绕着一些定义较为宽泛的政治信仰而团结起来。这种团结并非基于种族/民族认同、宗教、性别/性取向，也并非专注于某个特定议题。社会学家曾批判过这种群体可能采取单一抵抗运动，但鲜有关于跨议题斗争中团结一致的案例（Hall and Du Gay 1996）。尽管他们仍然沿用一些较为传统的行动主义方式，例如占领运动和街头游行，但该群体成员更加关注其内部实践和文化。一系列与政治犯支持、动物权利、自行车权益倡导、食品正义、住房权利等相关的实践活动，都体现了该群体成员共同的激进议程和集体认同构建，而这种构建基于对社会不平等根源的认知和行动。

为了解答关于问责制的问题，我运用了历史文献，采访了行动者，并分析了独立出版物。此外，我还将自身的轶事经验作为一种自传式民族志形式，来阐明我的研究。我相信，这种多管齐下的方法将有助于更全面、更深入地理解问责制以及转化性正义在激进左翼亚文化中的运用。

历史背景

通过正式的问责流程来运用转化性正义或许是一种新现象，但其背后存在的性别问题却贯穿了整个新左翼社会运动。尽管我研究的亚文化并非直接源于这些社会运动，但它却是新左翼社会运动发展轨迹的一部分。后公民运动中发展起来的历史和意识形态对该社群的持久性和韧性至关重要。这种亚文化是文化第三波浪潮从争取平等转向激进政治的产物。它体现了对特权和权力交织的认知，这要求人们进行反思并将信念应用于实证研究。

后民权运动时期活动家的革命原则激励着这个群体，他们“与主流民权团体不同……寻求的是美国社会本身的结构性变革”（Bond 2000）。如今，一些同盟团体仍然与那一时期的政治犯保持联系并为其发声，其中包括学生非暴力协调委员会的贾米尔·阿卜杜拉·阿明、黑豹党的穆米亚·阿布-贾马尔以及争取民主社会学生会/‘气象员地下组织’的戴维·吉尔伯特。革命活动家对社会正义的关注延续至今，他们渴望文化变革，并认识到各种交叉性压迫的存在。

为了更好地理解组织者面临的问题，我研究了三个采用预示性政治策略、混合性别、面向青年、关注多个议题的行动主义激进团体。我运用自传、历史记述和访谈，梳理了一段简史，探讨了女性在学生非暴力协调委员会、黑豹党以及地下气象员组织中的角色。重要的是要考察当时的议题是什么，行动者如何应对这些议题，以及这些应对措施如何影响了各自的社会运动。

该场域的当代文化

这种亚文化是由无政府主义者、自由素食者、朋克、学者和各种左翼活动人士交织而成的网络。参与者自称为“社群”，这在象征意义上为运动奠定了基础，暗示着持久性、一致性和凝聚力。诸如无政府主义书展之类的活动强调，参与本身就是一种加入“我们社群”的方式，而社群的凝聚力对于确保诸如免费托儿服务和更安全的空间政策等便利设施至关重要。社群成员资格是一个灵活的概念，没有明确的定义，也没有任何必要的标志或资格。因此，社群是一个反映环境背景变化和个体经历转变的过程。

参与者将分散的城市区域称为“社区”，以此唤起人们对传统街区或小镇的亲密感和空间内涵的联想。这些社区中的素食餐厅、自行车店、集体居住空间和前卫书店，构成了城镇的有形边界，在某种程度上自成一体，自给自足。定期的面对面交流和共同的文化标志对于人际关系的建立至关重要。

基于特定语境的“地方特殊性”与更大的全球网络相连（Featherstone 2005，Shepard 和 Hayduk 2002，Robinson 2008）。由于亚文化存在于地方层面，却又是社会正义“团结网络”的一部分，因此“社群”一词被用来指代激进左翼行动主义的更广泛精神（Pickerill/Chatterton 2006）。对不同受众而言，“我们的社群”有着不同的含义。“从纽约到希腊，去他妈的警察！”这样的抗议口号正是对这些网络连接和与现有权力结构相关的共性的一种认可。

有些社群团体是特定地域环境的产物，而另一些则是跨国联系和跨利益群体共同作用的结果。发生在地方之外的问题被带入到地方语境中。联盟和组织将全球范围内的团体和社群联系起来。诸如无政府主义黑十字联盟（ABCF）、食物而非炸弹（FNB）和有色人种无政府主义者（APOC）等团体或“社会运动组织”以去等级化的附属形式存在，并设有地方分支机构；它们就像一个无政府主义特许经营机构，为世界各地城市的相关团体提供统一的标签。这些组织通常会有一本手册或一套基本原则，阐述其意识形态基础、具体议题和行动方法。此外，还有一些规模更大的、涵盖范围更广的“运动产业”，例如囚犯权利、动物权利和反战运动等。

不同社群之间的联系可能包括合并、分裂、合作与冲突。个人往往拥有多个社群成员身份，通过组织活动、友谊和性关系彼此联系。社群之间可能共同组织活动，或作为其他社群的盟友，协助筹款或组织慈善活动。正如一位有色人种酷儿女性活动家所说：“朋克圈、酷儿社群、社区组织、社会活动、有色人种群体……所有这些社群对我来说都是相互联系的”（King 2012: 96）。

虽然加入社群能提供结识新朋友的人脉网络，但网络的庞大也可能导致某些同道团体之间缺乏联系。同样，网络中的成员也可能并不熟悉甚至从未见过所有其他成员。层层叠叠的社交和同道团体关系会导致人群集中在网络的某些区域。各个小组之间相互联系，关系随时间推

移而变化，而且没有单一的中心组织或团体，这使得激进社群“难以控制、监督和监管”（Pickerill and Chatterton 2006: 740）。

朋克

激进行动主义文化根植于“自己动手”（DIY）理念，强调行动者的自主性和变革社会的潜力。DIY方法是行动者将激进左翼政治理念应用于自身行为和实践的一种途径。组织者将自我教育视为一种解放力量。这种亚文化重视阅读、研讨会和信息商店（即摆放书籍、杂志和小册子的聚会场所）。“技能分享”是指行动者互相学习实用技能的聚会，大家通常通过实践来获取知识。虽然没有报酬，但组织者之间经常会进行技能交流。例如，缝纫工作坊、自行车组装、丝网印刷和转化性正义工作坊等。

各种元素的融合造就了一种多元化的品味文化和生活方式，它既契合参与者的个性，又体现了其所处的环境和政治伦理。如果说朋克社群有专属的配乐的话，那非朋克音乐莫属了。历史上，朋克音乐融合了保守和自由两种政治观点（Moore 2010）。当被问及政治立场时，朋克活动家们常常会提到某些音乐或乐队是他们投身政治活动的原因。朋克音乐本身就具有民主和DIY的特质，鼓励所有人参与。参与者将各种非传统的文化实践融入日常生活，例如创作独立杂志或举办派对来支持某项事业，这些都体现了他们对政治不满的表达。朋克乐队举办慈善演出来筹集诉讼费用、社区空间租金以及其他各种项目资金也十分常见。

更具体地说，在女权主义和酷儿相关的社群中，20世纪90年代的朋克亚流派“暴女”（riot grrrl）仍然很受欢迎。暴女运动植根于第三波女权主义，是作为对传统男性主导朋克的回应和衍生（Gottlieb and Wald 1994, Siegel 2007, Piano 2003, Kearney 1997, Leonard 1997, Wadkins and Konkiel 2011）。该亚流派毫不掩饰地展现女性特质，并拥有明确的政治兴趣和目标，在亚文化内部以及女权运动中都积极发声。在意识形态上，暴女承认交叉性身份和不平等现象，但是该亚文化仍然基于一种传统的白人音乐形式，将参与者限制在特定文化群体中，并延续了朋克音乐无意中存在的种族排斥（Piano 2003, Schilt 2005）。

尽管朋克在激进文化中扮演着至关重要的角色，但有些人试图与其断绝关系，以摆脱其潜在的种族限制，以吸引更多非朋克群体。朋克群体以白人和年轻人为主。朋克美学中破烂的衣着和蓬乱的头发刻意地象征着混乱和反抗。正如赫布迪格对20世纪70年代朋克的研究所示，这种美学持续表达着“对主流文化和意识形态实践的对抗”（Willis，1977，第xiii页）。在激进亚文化中，朋克可能会阻碍非朋克群体的参与，尤其是在中产阶级化的社区。这种“对抗”的表达方式含糊不清，其目的也不明确，特别是对于那些不了解这种亚文化符号的人来说。为了实现种族和民族多元化，朋克采取的策略包括有针对性地宣传活动、改变慈善演出中的音乐类型、优先考虑与社区的关系，以及刻意跟那些与朋克或朋克音乐无关的激进团体建立联系。

人口统计数据

激进亚文化群体的构成反映了城市青年文化面貌的变迁。大多数参与者年龄在20岁出头到30岁中期之间。他们既非典型的男性也非典型的女性，部分成员认同自己是酷儿或性别非二元人士。与以往对社会正义活动家的研究类似，许多参与者来自中产阶级或工人阶级家庭（Ibrahim 2011, Ruth 2005, Bagguley 1995）。参与者的种族和民族构成较为多元化，例如APOC（有色人种无政府主义者）和POC（有色人种）杂志项目等团体。然而，总体而言，白人活动家的比例过高（Holland, Fox, Daro 2008）。种族和民族多样性的缺失一直是激进亚文化群体关注的问题（Freeman 2009）。参与者很少信奉宗教，也没有特定的宗教信仰；然而，占星术和巫术等形式较为流行，尤其是在LGBTQ群体和女性活动家群体中。一些个人和团体甚至创造了自己的塔罗牌，对牌面进行了政治化的解读，例如《集体塔罗》（The Collective Tarot）、《下一世界塔罗》（Next World Tarot）和《慢呼喊》（Slow Holler）。

参与者正步入成年，不再拥有青少年时期那种无需为生计担忧的自由。有些人可能拥有汽车，但更多人选择骑自行车出行，并依赖公共交通工具。其中一些积极者是学生或应届毕业生，他们获得父母的支持、奖学金和助学贷款。常见的有利于激进政治活动的雇主包括素食餐厅、健康食品市场、女权主义和酷儿性用品商店，以及各种非营利组织。一些人则从事非正规经济活动，例如遛狗、提供替代疗法和性工作，这些工作能够提供自主性和灵活的时间安排。

许多参与者就读于或隶属于学术机构，并接受过一定程度的大学教育。如前所述，大学校园内已建立起各种行动团体，既是行动主义亚文化的资源，也与该亚文化有着密切联系。大学生有机会尝试各种另类文化实践（Ibrahim 2011）。他们在课堂、社团和其他校园活动中建立的友谊，构建了新的社交网络。无论在课堂内外，学生们都会接触到对现状和主流观念的批判，以及新思想和新思维方式。

虽然有些人可能与父母同住或住在自己的公寓里，但许多人与同伴活动家合住、或住在集体/共享房屋中。有些人则参与非法占用或占领空置房产。在条件允许的情况下，较大的居住空间会兼作会议、活动和多功能场所。也有一些房屋专门用作居住和社区空间的双重功能。

该社群成员很少结婚或生育子女。这部分是由于年龄因素，但也与意识形态和生活方式密切相关。婚姻，无论是异性恋还是同性恋，都意味着与国家建立联系，其根基在于宗教，并维护着传统的性别角色。该社群奉行多种性关系，包括多伴侣关系、多性伴侣关系以及 BDSM 等。因此，该亚文化群体中的一些人将婚姻视为融入一个社会不公文化的过程。

[image]

为人父母也限制了参与。对于有孩子的人来说，参与活动要么不方便，要么根本无法进行。深夜会议、夜间活动以及可能涉及激进的非法活动都需要投入大量的时间，通常并不适合儿童。我曾经参与或合作过的团体在组织活动时，并非有意排除儿童，但我们却无意中忽略或没有考虑到这一点。为了解决这个问题，一些活动人士撰写了《别让你的朋友掉队：在社会正义运动和社区中支持家庭的具体方法》一书，书中提供了将活动和家庭生活相结合的不同途径。一些团体已经意识到这些限制，并正在调整自己的做法，以更好地照顾父母和孩子，例如无政府主义书展就提供儿童照护和适合儿童的工作坊。

[image]

上述这本书（Don't Leave Your Friends Behind: Concrete Ways to Support Families in Social Justice Movements and Communities）：https://z-library.sk/book/18233948/0c38c8/dont-leave-your-friends-behind-concrete-ways-to-support-families-in-social-justice-movements-and-c.html

[image]

访谈

由于我研究的是一个鲜为人知的社会进程，且涉及一个独特的群体，因此我的访谈并非旨在追求统计学上的代表性，而是为了阐明这些进程以及行动者的经历。从数量上看，行动者尝试过多少进程、完成过多少进程，以及参与人数多少，目前尚不得而知。2018年4月至9月，我采访了12位受访者，以收集有关性别、人际互动和转化性正义模式的数据。其中四位受访者是我在参与不同行动团体时结识的。其余八位受访者是通过滚雪球抽样的方式招募的，他们是通过联系已知的行动团体和社交网络招募的。参与者需满足以下条件：年满18周岁，愿意接受录音，并且直接或间接地参与过问责进程。

为了确保受访者言语的使用和语气的准确性和具体性，我对访谈进行了录音。访谈时长为45分钟至三个半小时不等。所有访谈均以英语进行，受访者均身处美国。虽然在加拿大、澳大利亚、英国、法国、德国和其他国家也有许多团体和个人参与其中，但我不想让文化差异和刑事司法体系的差异问题干扰这项研究。由于活动人士经常搬迁，因此我进行了10次电话访谈和2次面谈。由于我没有记录受访者的姓名，他们保持匿名，因此伦理审查委员会加快了我的申请审批。我使用化名是为了区分不同活动人士的声音。

我采访的12人中，人口统计信息各不相同。虽然他们不能完全代表左翼活动人士，但很可能代表了参与转化性正义的活动人士。除一人外，其余人在开始参与社会活动和问责进程时都处于20至30岁之间。在种族方面，11人自认为是白人，1人自认为是亚裔和中东裔混血。

在亚文化群体中，性别和性取向比主流社会更加流动和实验性。活动人士认同自己为非二元性别或性别不符合者并不罕见。“顺性别”（cisgender）一词指的是认同出生时被指定的性别，它是活动人士常用的术语，用来与“跨性别”（transgender）一词在语言上保持相对平衡。两位受访者自认为是顺性别男性，两位受访者自认为是性别酷儿或非二元，一位是跨性别女性，其余七位是顺性别女性。关于受访者的性取向，三位自认为是异性恋或“基本异性恋”，一位是双性恋，八位是酷儿。“酷儿”意味着他们的性取向不符合二元性别框架。

我向受访者提出的是开放式、一般性的问题，广泛询问他们在参与问责程序前的激进主义行动经历、问责程序本身及最终结果。随后，我进一步追问流程形式、诉求内容及社区角色等具体问题。我还请他们评估问责程序是否成功，以及是否对此有所遗憾。

受访者在众多程序中承担了不同角色：其中八人担任调解人，负责连接幸存者与施害者；两人是幸存者，六人参与幸存者支持团队；一人是施害者，三人参与施害者支持团队；另有一人虽未在任何程序中担任正式角色，但密切关注相关进程并撰写了广为流传的主题刊物。

可以理解的是，参与过这些问责流程的人可能不愿参与我的研究。研究社会运动的学者经常令活动人士失望，他们觉得访谈不过是"研究行程表上有待逐一勾选的项目"，事后鲜少被联系，也得不到最终发表的文章或文件（Kempson）。法律层面也存在诸多问题，例如活动人士公开指控特定个人，以及诉诸肢体报复和暴力手段。部分受访者要求我口头确认其匿名性。

与此同时，也有许多从未有机会表达观点或经历的人主动寻求访谈。其中不少人参与运动已多年，此后选择不再回溯当时的历程。我们的访谈为部分人提供了宣泄不满或重新审视抗争历史的空间。另一些仍在坚持抗争的人则希望通过访谈能为汇集抗争实践的集体知识库贡献力量。

[image]

小册子

小册子（Zines）文献在社区中扮演着至关重要的角色。发音类似于"magazine"的第三个音节，ZINE是一种类似于宣传册或手册的DIY出版形式，由个人、集体或合作团队创作。在《偷来的马克笔革命》一书中，小册子作家亚历克斯·雷克将ZINE定义为"实体印刷的自出版创作，可由单张纸或多张纸组成，通常用订书钉装订"（Wrekk 9）。虽无统一标准，但多数杂志采用标准纸张尺寸（8.5×11英寸）对折而成。独立刊物通常采用复印制作，"但也可能使用胶印、凸版印刷、油印或里索印刷"，"发行量可从1份到数千份不等，但通常低于1000份"（Wrekk 9）。

小册子在形式和内容上都体现着DIY精神。其版式设计是为有意展现这种自制特质与创作过程。小册子"融合了写作、艺术、制作乃至研究等多项技能"，使创作者能够"运用文字之外的多种形式讲述故事"（Wrekk 13, 19）。多数小册子采用剪贴美学，仿佛创作者将文字、图像等素材从原始载体中剥离后重新拼贴。文字常模仿打字机字体，被分段裁剪后粘贴于页面。创作者可能根据主题协调字体，添加手写部分，并刻意变换风格。图像或经剪贴拼贴于页面，或以手绘呈现。风格的组合与层叠揭示出多方面的含义。

由于强调艺术探索与非正式教育，这类文化极具生产力，不断创造并传播共享的知识与历史。杂志内容涵盖"从食品政治到二手购物再到为人父母"等所有可想象的主题，且往往对活动家的经历进行反思（Piepmeier 2）。作为参与政治亚文化的重要载体，独立刊物常包含DIY或"操作指南"类内容，如纯素烹饪、城市园艺、个人健康或集体组织创建等。尤其在酷儿群体与女性主义者中，独立刊物已成为自我表达与经验共享的重要平台。

个人或"分销商"负责小册子的流通。“分销商"通常是小型爱好者邮购店、网店，或偶尔在展会活动中销售杂志及其他物品的集市摊位"（Wrekk 11）。活动组织者会在现场设置"摊位"展示这些小册子，即团体获得的桌位空间以陈列印刷品及其他团体资讯、贴布、徽章和传单。这些物品通常免费提供、接受物物交换或以低于5美元的价格出售，所得款项用于覆盖印刷成本或为团体筹集资金。

小册子作者鲜少盈利。尽管纸质印刷品仍在创作并广泛流通，但大量内容现已转至线上。当前很多小册子都可通过PDF格式在线获取，或从分销商及存档网站购买。此外，巴纳德学院和纽约市立大学布鲁克林学院现均设有校园杂志图书馆。

小册子作者们正致力于在亚文化中实践修复性与转化性正义模式。由于该亚文化普遍反权威且对抗刑事司法体系，活动家们正利用现有资源与自身文化背景，探索更具伦理性的正义模型。相关政策讨论已遍及各类活动、会议、杂志、邮件及博客文章。

为开展这项研究，我通过121本独立刊物来考察活动家们的经历。其中不足半数为纸质版，其余均为在线找到的流通的PDF格式。我参与活动期间收集了大量印刷版册子，这些小册子在亚文化圈内广泛流

通。其中包括布鲁克林本地及女性主义杂志节的刊物、无政府主义书展或有色人种杂志项目巡展等活动中的组织摊位刊物，以及朋友制作的杂志。其余刊物购自纽约蓝袜书店、费城木鞋书店、AK出版社等激进出版机构及网络杂志分销平台。PDF版本则通过费城"愤怒者"、"支持纽约"等转型正义组织官网，以及酷儿杂志档案项目等在线杂志库获取。

小册子可能具有地域性特征，刊载本地化资源和资讯，却也跨越国界传播。我主要关注在美国流通的小册子，但这并不意味着所有小册子都由美国人撰写的。我将研究范围限定于英语小册子，因其流通最广；不过我也确实发现了西班牙语、德语和法语版本的小册子，内容涉及性别歧视、同意权及转化性正义等议题。作为"支持纽约"组织成员，其他国家的活动家会通过Skype与我们讨论团体运作流程；作为"For the Birds Collective"成员，我们扫描小册子寄给海外的团体。信息的流动使得国家边界难以成为限制与划分的标准。

我所使用的小册子样本并非旨在代表小册子的整体数量，而是评估活动家亚文化中组织者围绕性别相关议题撰写并传播的册子内容。我将所选的小册子分为四大主题：1）性别歧视，2）同意和性侵犯，3）男性团体，4）转化性正义与问责制。其中多数为合辑，由多人或团体共同撰写，部分文章会出现在多本册子中。部分刊物属于系列作品，我仅选取涉及前述主题的期号，或仅使用能获取的期号——因"小册子出版发行极不规律"（Freedman 2018）。许多刊物的来源或作者不明，仅署名昵称或完全匿名。

我收集到的第一类也是最普遍一类小册子的主题是关于激进主义中的性别歧视问题的。这些杂志探讨了诸如会议结构、性别歧视与COINTELPRO（反情报计划）计划、性别与暴力的关联等议题。其中部分属于个人杂志（perzine），即"聚焦作者生活、观点与思考"的刊物（Freedman 2018）。另一些则是应对性别歧视的通用指南。《超级快乐无政府主义趣味页》和《近期占领行动纪实》等刊物配有漫画插图。在探讨性别歧视的小册子中，有两本尤为值得关注：《首张的7寸唱片更胜一筹》后来被学术期刊《女性与表演》收录；而《她为何对你们的起义漠不关心》则因回应起义派无政府主义者的行动，在亚文化圈引发巨大争议。

性别歧视主题杂志标题（符号表示实体书^或PDF*）

- 背叛：对无政府主义亚文化中强奸文化的批判性分析^
- 脑扫描第27期：十则故事^
- 脑扫描后记^
- 打破枷锁：反父权主义读本^
- 兄弟们退后*
- 危险空间：暴力抵抗、自卫与反性别起义斗争*
- 别当混蛋*
- 厄里倪厄斯：无政府女权主义油印第2期^
- 厨房实录：性别歧视、无政府主义与男性*
- 性别化空间，第一卷^
- 我怎么可能是性别歧视者？我可是无政府主义者*
- 我们如何亲吻：舞池中的特权*
- 我的女性主义宣言：致男性的呼吁*
- 没有安全屋：左翼中的父权制（四部曲之二）
- 论近期占领的运动^

- 半斤八两：给无政府主义男性的女性主义理论^
- 你想创建女权主义集体吗？^
- 首张7寸唱片更胜一筹：我如何成为前朋克*
- 超级快乐无政府主义趣味专栏#3*
- 思考并死于思考*
- 猎杀吸血鬼：人际关系与团体中的操控术^
- 姐妹情谊何在？如果忙于内斗，我们便无力对抗父权*
- 当女性发起反击*
- [image]为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力 *
- 她为何对你们的起义漠不关心^

我创建的第二个小册子类别是专门针对同意和性侵犯的。其中虽有 On the Table 和 Everything. Is. Fine. 等个人杂志，但多数是关于自我保护、合意性行为及开展同意权工作坊的指南。《Learning Good Consent》堪称亚文化圈最受欢迎的册子之一，至今仍频繁出现在各类杂志节和活动中。

同意与性侵犯主题的小册子（符号表示实体书^或**PDF***）

- 防止性侵犯的 DIY 指南*

- 一辆名为“同意”的有轨电车：性同意与愉悦的策略*
- 又名：如何搭讪某人^
- 先问！性侵支持者、幸存者与施暴者的资源指南*
- 《黑屏》第3期^
- 同意是我的操作系统的一部分*
- 不要互相强奸！同意是一个社群议题*
- 一切。都。好。第1期，第1卷^
- 搞砸了：在性积极酷儿圈中遭遇性功能障碍*
- 嘿辣妹！派对场合中的同意、沟通与边界设定^
- 如何打造专属社区的参与式激进同意工作坊*
- 我正在经历漫长的似曾相识 #1*
- 学习良好的同意^
- 宝，我们来谈谈‘同意’吧*
- 也谈‘同意’^
- 畅谈：激进化性行为、同意与人际动态的女性主义沟通*

- 听着，混蛋，你可能误会了：没有我明确而充分的同意就绝不允许！
- 我的身体，我的界限，我的愉悦，我的选择：青年积极性教育手册*
- 未经我同意绝不允许！（混蛋！）*
- 摆上台面：我的性侵经历*
- 净化#3 性侵幸存者故事集^
- 性暴力不止发生在街头：触摸我之前请先询问^
- 沉默＝死亡*
- 聪明辣妹：女性、酷儿与跨性别者性健康积极小册子#1^
- 支持^
- 女性自卫术#2：生存故事与策略*

我收录的第三类小册子是由男性团体撰写，和/或专门面向男性行动者的。《费城兄弟会》（Philly Dudes Collective）在我还是“支持纽约”（Support New York）和“为了鸟儿”（For the Birds Collective）成员时，是一份特别受欢迎的杂志。还有一篇未在此列出，因为它只收录在后来出版的《革命始于家庭》（The Revolution Starts at Home）一书中，那就是“挑战男性至上项目”的文章《变革终将到来时感觉如何？：男性至上、问责制与转化性正义》。

男性团体主题小册子标题（符号表示纸质版^或PDF*）

- 负责任的性行为初学者指南（针对男性）^
- 走出'男性'：对亲女权主义男性团体的批判性反思*
- 打击强奸：处理我们的烂摊子*
- 男性气质^
- 男性可以阻止强奸*
- 男性在女权主义斗争中的角色*
- 男人直言谈男性与性别歧视，第一期*
- 男性摒弃强奸行为^
- 男性、性别歧视与阶级之战^
- 疗愈之路：一本写给男性的反性别歧视手册*
- 疗愈之路：男性反性别歧视手册，第二期*
- 社会排毒，第1期：反性别歧视男性的资源^
- 费城兄弟团：第一年（零半）^

最后一类小册子是关于转化性正义的。这类小册子包括个人杂志、转化性正义指南和评论。其中一些明确提及了某个具体的、有名有姓的活动家。正因如此，我从《关于Xxxxxxxx的zine》中删除了该活动家的姓名。虽然这个名字是此人使用的化名，但他的名字广为人知，足以构成指代。其他一些小册子，例如《宝，我是个无政府主义者》和

《脑部扫描》，在内容中提到了某个具体人物，因此在任何引用中，我都不会提及被指控虐待或伤害的人的姓名。在这些小册子中，《支持》、《迈出第一步》、《性别压迫》、和《我们都是幸存者》尤其常见。

转化性正义与问责制杂志标题（符号表示纸质版^或PDF*）

- A级团队的任务：一本关于意识觉醒和社区责任的小册子*
- 创伤后自我护理的极简指南^
- 挺身而出的初创行动：以转化性正义应对性侵犯*
- 一个没有性侵犯的世界*
- 问责流程充满了该死的健全中心主义！
- 问责制^
- [image]为我们自己负责 - 打破反贼圈子中关于攻击和虐待的僵局：超越米兔S09E04 *
- 问责流程入门：如何准备和推进问责流程*
- 就当他们是人：关于加害者问责的不同视角 *
- 宝贝，我是个大男子主义"无政府主义者"^
- 美丽、艰难、有力：通过转变性正义终结性侵犯*
- 不为人知：直面亲密关系中的情感虐待^

- 苦涩与愤怒：做一个“糟糕的幸存者”
- 脑部扫描#21：不可调和的分歧^
- 脑部扫描 #26：那么，你和‘微观世界’到底是怎么回事？
- DIY问责制：如果他们不主动承担责任 —— 那我们就自己来^
- 解决我的难题，第2期*
- 为了您的安全和保障 ......*
- 性别压迫；虐待；暴力：有色人种进步运动中的社区问责^
- 天知道我现在有多痛苦：支持和无政府主义社区^
- 骗局#12：女权主义与疗愈^
- 如果一名男子在纽敦犯下强奸罪，而没有人知道该如何处理......*
- 掌握在我们手中：运用社区问责制方法应对性暴力、虐待和压迫 #1*
- 归根结底 #2：关于性暴力、问责、同意和疗愈^
- 归根结底：关于社区和集体应对性暴力、虐待和问责的反思、故事、经验、评论和想法^
- 让空间更安全^

- 避难所 避难所：一本变革性的正义杂志* （注：希伯来语Miklat 字面意思是「避难所」，并有「接纳」、「收容」...「圣洁之地」的意思）
- 迈向变革性正义文化^
- 我的朋友是加害者：我该怎么办？
- 言尽于此 #3^
- 我们自己的回应：创建更健康的社区^
- 争执：关于幸存者自决、直接行动的故事、更安全空间、以及撕碎父权制的策略*
- 关于 Xxxxxxxx^
- 挽救：激进社群中的性别暴力*
- 非礼勿视，非礼勿言，非礼勿听：关于性侵犯的文章和问题^
- 烧掉“社会正义教会”：对身份政治、网络声讨文化及其他国家主义思维模式的3种批判*
- 幸存者策略*
- 支持性侵幸存者*
- 生存、赋能、反抗：纽约市性侵幸存者资源指南^
- 承担风险：实施基层社区问责战略^

- 迈出第一步：给那些被指责有虐待行为的人的建议^
- 破碎的茶壶*
- 我们村里的铁锤：左翼中的父权制（三/四）
- 革命始于家庭：在行动主义社区中直面伴侣虐待^
- 这不仅仅关乎我们和谁上床（以及谁和我们上床）^
- 关于社区对亲密暴力可能采取的应对措施的思考（重温版）^
- 关于围绕亲密暴力开展社区支持的思考^
- 厌倦了纸片人^
- 转化性正义和/或伤害*
- 我们都是幸存者，我们都是施害者 // 当有人告诉你你侵犯了他们的界限、让他们感到不舒服或实施了攻击时，该怎么办？
- 那么强奸犯呢？无政府主义对犯罪与正义的看法*
- 我们该如何应对？一本关于社区对性侵犯事件反应的杂志，第2期*
- 我们该如何应对？社区对性侵犯的激进应对，第3期^
- 发生伤害时该怎么办*

- 被公开指责后该怎么办：简要指南*

- 猎巫：激进主义社区中的心理健康与性侵犯应对*

我阅读了所有列出的小册子，并根据历史研究中提炼出的特定主题对内容进行了分类整理。内容被划分为以下议题：组织与安全文化、同意与性关系、更安全的空间、虐待与伤害、幸存者与施害者、处理流程、成功经验与困境、暴力的使用、来自亚文化内部的批判，以及由此引发的行动主义模式转变或退出。在文献评估中，我力求尽可能准确地呈现作者的背景与情感，以及亚文化圈子中流传的信息。

此外，我还借助亚文化中的其他类型文献来深入探讨转变性正义实践。如前所述，部分独立刊物已增补章节与文章后重新出版成书，例如《学习良好同意：关于健康关系与幸存者支持》《革命始于家庭》以及《多丽丝百科全书》。此外还涉及若干亚文化相关的无政府主义报刊，如《犯罪思想》《第五权》《废奴主义者》。部分转变性正义团体已开发出流程化课程与工具包。研究材料还涵盖艺术作品与漫画、组织宣传单页、活动手册、安全空间政策、博客文章、组织官网及相关文献。

[image]

第三章 新左翼运动的历史模式

> 若不尊重他人，便无从谈爱；若不践行政治团结，便无资格呼吁政治团结。这些品质并非凭空产生，而是需要日复一日地付诸实践。—— 阿萨塔·沙库尔

由于新左翼运动"植根于美国经验与语言"，它们同样映射出这些权力差异（Flacks 2013: 840）。激进左翼行动主义内部对过往运动的内在文化缺乏全面认知。无论过去还是现在，组织者往往将人际关系视为私事，认为其独立于事业之外或者不如事业重要。然而父权制与性别歧视正是性别融合运动中动员女性的主要障碍（Horn 2013, Kuumba 2001）。为阐明这些动态，我将考察新左派的三场社会运动，分析它们如何概念化这些议题、如何应对问题，以及如何影响整

个社会运动。

我专门考察了学生非暴力协调委员会（SNCC）、黑豹党以及民主社会学生会/地下气象组织（SDS/WUO）中基于性别的动态演变史。在探讨"代际地下运动"与社会运动的交叠时，斯图尔特·霍尔明确指出"民权运动"（SNCC）、"黑人权力运动"（黑豹党）和"校园反叛"（SDS）均存在于文化辩证法的"行动主义一极"（2007: 160）。尽管这些相继出现的运动致力于反抗当时的规范和条件，但它们同时也深深植根于各自时代的规范和条件之中。

SNCC、黑豹党以及SDS/WUO等组织，最适合置于其时代背景中进行审视。1960至1980年间，美国女性的生活经历了剧变。许多女性被教导要"接受男性的主导地位，并将自己视为 …… 男性的帮手"（Jennings 2001: 146）。在之前的1950年代，社会将女性的价值定义为婚姻与生育，这被视为对抗共产主义和冷战的"国家议程的组成部分"（PBS 2003）。尽管女性占大学生总数的32%（拉瓜迪亚与瓦格纳档案馆），但当时盛行一种玩笑说女性"上大学是为了获得'夫人'（发音为M.R.S.）学位，即丈夫学位"（PBS 2003），且仅有33.9%的女性参与平民劳动力市场（Toossi 2002）。到1980年，女性占大学生总数的51.8%（NCES 2010），占平民劳动力比例达51.5%（Toossi 2002）。同期围绕性话题及性骚扰/性侵的公共话语也发生了剧变。

SNCC、黑豹党以及SDS/WUO的活动家们深陷于这些不断变化的文化规范之中。黑豹党的埃琳·布朗曾指出："我们身边的人并非都来自革命天堂"，这揭示了在日常生活物质现实中践行意识形态的艰难。将意识形态付诸实践意味着活动家既要回应当下现实，也要肩负创造理想世界的使命。他们正在塑造一种推动社会变革的文化，"揭示那些与之对抗的正式机构背后的深层结构"（Brotherton and Barrios 2004:49）。

本文无意撰写结论性史料，而是旨在系统梳理这三大社会运动中性别、性与组织运作的交织关系。具体而言，我归纳出四大核心主题：群体中女性的正式与非正式角色定位；性别如何影响组织架构（如分工与领导层配置）；群体内部的社会纽带与性关系；以及处理内部冲突与自我批判的机制。

学生非暴力协调委员会（SNCC）

学生非暴力协调委员会（SNCC，发音为"snick"）成立于1960年，旨在支持学生反对种族隔离的行动（Polletta 2013）。南方基督教领袖会议（SCLC）与种族平等大会（CORE）等组织在萧尔大学召开会议，旨在将学生分支纳入其体系。SCLC创始成员、萧尔大学会议组织者埃拉·贝克曾批评该组织等级森严且父权制色彩浓厚（Abu-Jamal 2004, Greenberg 1998）。会议期间，她建议包括朱利安·邦德和约翰·刘易斯在内的学生建立自己的自治团体。她期望学生们"不仅要保持热忱、理想主义和独立性，更要秉持'以群体为中心而非以领袖为中心'的组织模式"（吉丁斯 2007: 274）。

SNCC作为民主组织发展起来，层级结构极简。该组织设有主席及若干专业职位与顾问，但本质上是由工作人员和当地民众组成的网络，在东南各社区独立运作（Urban 2002, Anderson-Bricker 1999）。该组织早期行动包括静坐抗议和选民登记。工作人员与其他活动者及当地居民建立了深厚友谊。SNCC构想的"挚爱共同体"理念，被视为一种乌托邦式的预示性微观社会。他们通过让工作人员效仿当地贫困农村居民的着装与举止来强化这一理念 —— 例如穿着牛仔工装裤，女性尽量淡妆（Ford 2013）。

在规模最大的时期，SNCC拥有160名工作人员（Polletta 2013），其中女性人数远高于其他民权组织。该组织协调员珍·威利坦言："我从未想过SNCC会有这么多女性，这么多黑人女性，因为在我参与过的所有政治团体中……男性都占据压倒性多数。无论黑人白人——但都是男性"（Veterans 2004）。部分SNCC成员认为当地黑人男性参与度较低，因他们面临当地白人实实在在的人身威胁。CORE与SNCC成员哈迪·弗莱指出："男性总是最后进入教堂的，因为他们一直在外侦察局势，卡车里备有武器，本质上是抵御当地白人至上主义者的安全保障"（Veterans 2004）。

尽管个别文献将女性待遇描述为"低于男性"（Urban 2002），但多数研究认为该组织奉行性别平等原则（Veterans 2004, Fleming 1993, Carmichael 2003）。如果有的话，SNCC 将传统上与女性相关的任务视为优势而非劣势。当地黑人女性既是"替代性母亲形象"，又是"激进的 ... 直言不讳的 ... 且甘愿承受磨难"的存在（Evans 1980: 53, 51）。她们"因智慧、坚韧、力量以及超越生活压迫本质的能力而受

到整个社区的敬仰"（Giddings 2007: 284）。该组织重视女性在家庭中的核心地位，并将这些理念融入组织建设。丽塔·沃克这样的女性"带着丈夫甚至孩子来到[自由]之家 ... 她将运动视为生命本身"（Veterans 2004）。迪安娜·纳什等组织者则在显怀期间持续参与运动。纳什成为"有力宣言 ... 证明女性身份不会限制其在运动中全面而重要的参与"（霍尔萨特 2012: 486）。

SNCC的组织与领导

埃拉·贝克是该组织的早期顾问，她指引了SNCC的"政治取向、道德观和组织原则"（Carmichael 2003: 305）。贝克深谙权力集中之复杂性，甚至她自身的"指导如此自然、温和且不显眼，以至于当时几乎难以察觉"（卡迈克尔 2003: 305）。她强调"草根"行动主义，主张成员并非"领袖"而是"组织者"，"他们源于组织工作本身——而非由上而下强加"（理查德森2015，福特2013）。SNCC成员常戏谑那些备受瞩目的同伴，例如因媒体曝光度过高的斯托克利·卡迈克尔就被戏称为"明星迈克尔"（Greenberg 1998: 129）。该组织采用共识决策处理重大事务（Cornell 2016），日常运作则"基于成员自主决策与直觉行事"（Anderson-Bricker 1999:50）。活动家们将相互信任植根于相互依存（King 1988），视彼此为"手足般的家人"（Holsaert 2012: 386）。

尽管SNCC主席始终由男性担任，但女性在民权运动中扮演着重要领导角色（Holsaert 2012, Greenberg 1998）。该组织鼓励男女成员都担任外勤秘书和项目主管。然而在实际工作中，女性承担着传统意义上的女性事务，例如打扫自由之家、文书工作和记录会议纪要（Urban 2002, Anderson-Bricker 1999, Giddings 2007, Evans 1980）。学生非暴力协调委员会组织者朱迪·理查森回忆道："只有女性负责记录会议纪要...男性们从不做这件事 ——朱利安[邦德]绝对不会记录。你知道，吉米·博尔顿也不做。"（Wiley 2007）。为此，玛丽·金、露比·多丽丝·史密斯·罗宾逊、米尔德里德·福尔曼和朱迪·理查德森等女性发起抗议，在执行秘书吉姆·福尔曼办公室门前静坐示威。理查森描述了福尔曼遭遇的"半认真半戏谑的静坐抗议 ……众人齐唱《我们绝不退缩》，高举写着'不公'、'正义降临亚特兰大办公室前绝不复工'的示威牌"（Holsaert 2012: 361）。此后，男女成员开始共同承担会议记录工作。

有人认为这种分工有其内在逻辑。由于环境危险，男性负责驾驶车辆 —— 这是风险最高的任务之一（Evans 1980: 77）。鉴于黑人男性与白人女性交往的禁忌以及来自当地白人的威胁，白人女性承担了行政工作。黑人女性则拥有更多“能力做决定并参与高风险的激进行动”（Kuumba 2001: 37）。与此同时，SNCC鼓励更多男性承担家务劳动。斯托克利·卡迈克尔和詹姆斯·福尔曼以身作则，亲自洗碗（Greenberg 1998: 147）和扫地（Wiley 2007）。SNCC开展的大量工作涉及与当地社区协作、建立人际网络及行政事务 —— 这些正是"社会普遍鼓励女性发展的能力"（Evans 1980: 46）。行政工作不仅限于打字，更包含大规模组织协调、会议管理及决策制定等职能。

SNCC内部关系

SNCC将自身定位为"挚爱共同体"，这种理念塑造了组织内部的人际关系。成员的私人生活与社会活动紧密交织。组织者乔伊斯·拉德纳指出，SNCC的"关系首先且最根本地由当前任务定义"（Greenberg 1998: 144）。即便在艰难的会议之后，组织者们仍会转向欢愉与放松。玛丽·金回忆道："会议结束后总有音乐相伴，啤酒与舞蹈持续至深夜，我们彼此间的基本情感会流淌和覆盖当日的激烈争论留下的伤痕"（King 1988: 451）。来自外部的压力与危险反而强化了这些纽带。

[image]

延伸：https://iyouport.substack.com/p/f79?utm_source=publication-search

性关系在**SNCC**的发展历程中尤为重要。部分出身于"老左派"活动家和工会组织者的家庭成员，因担心引发复杂关系而回避与其他活动家的性接触（Greenberg 1998, Veterans 2004）。另一些人则认为建立关系"更容易尝试安定下来"，因为"性成为主要困扰…它既令人分心又令人不安"（Veterans 2004）。参与者们年轻气盛，挑战既有社会规范，且时刻面临风险威胁。对某些人而言，这意味着"和在场任何人都可能发生关系"（Evans 1980: 79），如楚德·帕姆·艾伦描述与韦恩·扬西相遇的情景： "我记得没超过60秒就问'嗨！想一起睡吗？'[笑声]而我当时有点保守，对吧？毕竟毫无性经验，简直吓坏了。后来他遇害了，我满心愧疚"（Veterans 2004）。活动家面临的危险被浪漫化，

并衍生出某种文化资本。布鲁斯·哈特福德和威利·B·瓦兹尔·皮科克在访谈中谈到，身为"自由斗士"会增添性感魅力，皮科克认为这促使更多人参与进来，因为"本地男孩们 ... 心生嫉妒 ... 于是其中几人开始 ... 加入进来"（Veterans 2004）。

跨种族性行为，尤其是白人女性与黑人男性之间的关系，曾引发巨大争议。当时，白人女性若被发现与黑人男性牵手或同乘一车，便可能面临人身威胁。有人认为跨种族性行为是构建"挚爱共同体"的组成部分，在"卧室亲密关系的具体现实中"挑战社会期待（Evans 1980: 79）。然而，将这些关系定义为社区建设的一部分时，也伴随着打破禁忌的压力 —— 必须"证明她们并非种族主义者"或证明她们对运动的坚定承诺（Veterans 2004）。

1964年自由之夏期间，性关系成为一个特殊问题并引发紧张局势。学生非暴力协调委员会（SNCC）在接纳或拒绝来自北方的女性志愿者时，部分依据她们的外貌特征（McAdam 1990）。部分白人女性与已有妻室或伴侣的黑人男性发生关系。当詹姆斯·福尔曼与身为黑人组织者的妻子米尔德里德离婚后，迅速迎娶了白人女子康斯坦西亚·罗米莉，此举昭示着"白人女性对黑人男性与黑人女性的婚姻关系毫无尊重 —— 这是每个黑人男性都心知肚明的"（Fleming 1998）。组织者格洛丽亚·理查德森·丹德里奇回忆，她耗费大量时间处理其他组织者的性关系问题。"成为性关系顾问是我不成文的工作描述中的另一项任务。这类问题常占据我过多时间，也最令我疲惫不堪"（Holsaert 2012: 29!218）。格温多林·卓哈拉·西蒙斯制定的"性骚扰政策，被某些男性同事曲解为'厌男症'"（Holsaert 2012: 31）。更有甚者直接禁止恋爱关系，或强行驱逐被视为滋事者的人员（Fleming 1998, Veterans 2004）。

性别、种族与内部纠纷

1964年秋，学生非暴力协调委员会（SNCC）的两名白人女性工作人员凯西·海登和玛丽·金匿名撰写了一份立场文件，题为《运动中的女性》，提交给SNCC韦弗兰会议。该文件列举了11个性别歧视的例子，包括“尽管有些女性 ...... 的工作年限与一些男性一样长，但领导层 ...... 却全是男性”，以及“SNCC中的任何女性，无论其职位或经验如何，都曾在女性人数少于男性的情况下被要求在会议上做会议记录”。这份清单并不完整，因为“只要运动中还有女性，就还可以继续

列举”，并指出白人特权也同样存在（Kuumba 2001）。一年后，在《性与种姓：一份备忘录》中，海顿和金再次反思了她们的行动经历，指出运动中缺乏关于性别的对话，并对运动内部的分工提出了质疑。值得注意的是，这两份声明都没有提及运动中的性与恋爱关系。她们将后一份文件寄给了全国各地不同的和平组织和民权组织的四十位女性组织者（King 1988，Greenberg 1998）。海顿后来写道，她撰写这些文章并非意在展现“内部的分歧”，而是意在展现女权主义的兴起，“因为学生非暴力协调委员会（SNCC）为她们的运动提供了一个范例 …… 为她们自身的运动提供了借鉴”（Greenberg 1998：145）。事后看来，历史学家认为《运动中的女性》一书是对日益高涨的黑人民族主义的回应，也是SNCC试图回归“理想社区”理念的一次尝试（Anderson-Bricker 1999：53），并且由于这些女性“感受到自身处境的岌岌可危”（Evans 1980：85），所以才采用匿名写作。

SNCC内部对该文件的普遍反应并不积极。许多白人女性与黑人女性在性别歧视的体验上存在分歧（Veterans 2004）。许多黑人女性组织者并未感到自己在SNCC中受到边缘化，部分原因在于"许多黑人女性工作人员比白人同行拥有更多权力、尊重和责任"（Anderson-Bricker 1999: 55）。另些人则认为白人女性"试图掌控办公室"（Fleming 1998），且性别歧视主要关乎白人女性的权益（Breines 1996）。对部分黑人女性而言，尽管组织内部存在沙文主义，但相较于种族问题，这并非首要议题（Anderson-Bricker 1999, Giddings 2007）。"她们拒绝接受以性别话语包装的黑人民族主义攻击"（Barber 2010: 105）。当性别歧视确实发生时，女性被要求展现坚韧，拒绝容忍并予以反击（Holsaert 2012: 481）。

1964年最初的立场文，正是斯托克利·卡迈克尔那句关于妇女在SNCC地位的著名言论的背景。在《自由之歌》中，玛丽·金指出该言论通常被断章取义，并重述了当时的对话。会议期间某晚，约25名SNCC成员会后在码头饮酒。卡迈克尔直视着我咧嘴大笑："女性在SNCC的地位是什么？"随即自问自答："女性在SNCC的地位就是趴着（prone）！"他仰头放声狂笑…… 我们全都笑得前仰后合。他那句粗俗的玩笑既荒诞又狂放，反而拉近了彼此距离 —— 因为即便在那刻，他也在自嘲自己的态度。凯西和我当时就觉得，直到1964年那篇匿名论文发表后仍深信不疑：斯托克利是当时最具洞察力的男性之一。"（1988:452） 相关记录表明，卡迈克尔提及1964年自由行运动期间围绕性问题的复杂状况时是在开玩笑，并非真正表达他对女性在运动中角色的看法。

1964年夏天成为SNCC的转折点。该组织日益呈现等级化、集中化与城市化特征。1966年，SNCC转型为全黑人组织，并逐渐走向激进化，包括在面对联邦政府失职时对非暴力原则提出质疑（McAdam 1985, Evans 1980）。尽管鲁比·多丽丝·史密斯·罗宾逊等女性确实晋升至更高领导层，但女性参与度整体下降（Kuumba 2001），而持续参与的女性则更"公开批判男性"（Giddings 2007）。1968年，弗朗西斯·M·比尔在SNCC内部发起第三世界妇女联盟（TWWA），该组织后独立并更名为黑人妇女联盟（Anderson-Bricker 1999）。尽管不如其他民权组织那样广为人知，SNCC仍深刻影响并塑造了后续学生运动，包括黑豹党和学生争取民主社会组织（SDS）。

[image]

黑豹党

1966年10月，鲍比·西尔与休伊·牛顿在加利福尼亚州奥克兰市创立黑豹党，该组织最初名为黑豹自卫党。黑豹徽章源自阿拉巴马州，最初是朗兹县自由组织（LFCO）的象征——该组织作为独立政党，旨在对抗全白人主导的民主党。学生非暴力协调委员会的斯托克利·卡迈克尔沿用了这一形象，此后早期黑人权力运动也纷纷效仿（Bloom and Martin 2016）。该组织最初的目标是通过武装自卫和监控警方活动，保护黑人社区免受警察暴行的侵害。西尔与牛顿制定了十点纲领如下：

1. 我们要求自由。我们要自己掌握决定黑人社区命运的权力。

1. 我们要实现我们的人民充分就业。

1. 我们要求终结白人对黑人社区的掠夺。

1. 我们要求体面的住房，足以供人类栖身。

1. 我们要为我们的人民提供教育，揭露这个腐朽的美国社会的真实本质。我们需要教授真实历史和我们在当今社会中所扮演角色的教育。

1. 我们要求所有黑人男性免于服兵役。

1. 我们要求立即终止警察对黑人的暴力和谋杀。

1. 我们要求所有被关押在联邦、州、县及市监狱的黑人获得自由。

1. 我们要求所有黑人被告在受审时，必须由其同族群体或黑人社区成员组成的陪审团进行审判—— 正如美国宪法所规定的那样。

1. 我们要求土地、面包、住房、教育、衣物、正义与和平。（加州大学出版社，2017年）

尽管军事化自卫训练始终是黑豹党的核心活动，直至该组织于1982年解散，但政治教育与社区项目 —— 如医疗诊所和早餐计划 —— 很快成为其组织工作的关键组成部分。在美学层面，该党标志性的黑色皮夹克、墨镜与自然卷发或非洲卷发造型，无不彰显着这种战斗精神。1967年，著名诗人兼前囚犯埃尔德里奇·克莱弗加入了党内领导层。据历史学家克莱伯恩·卡森所述："休伊·牛顿……是党的战略家。鲍比·西尔拥有领袖风范。埃尔德里奇·克莱弗则使该党在黑人知识分子及白人左翼知识分子中获得了公信力"（Nelson 2015）。鼎盛时期，该党在48个州设有分支机构，成员逾2000人（Brown 2018）。

1967年之前，黑豹党的成员以年轻男性为主。对早期组织者而言，该党是"一个能让底层兄弟参与进来的组织"，旨在"教育并政治化街区里的男性兄弟"（Newton 2009: 101, Bloom and Martin 2016: 95）。该党刊物《黑豹报》创刊号的招募启事宣称："这些兄弟是黑人男性的精英。他们肩负着保护和捍卫黑人社区的使命。黑人社区有责任为这些兄弟提供支持，这是为了我们民族的未来……黑人兄弟们！！！你们有责任向你们的妻子儿女、母亲姐妹说明党的纲领"（Newsprint Vault 2018）。男性作为第一道防线的定位，正是对奴隶制和吉姆·克劳法时期被剥夺的黑人男性尊严的重建（Bukhari-Alston 1995）。

最初，该党将加入的女性单独归为一个叫“小黑豹”的团体，但到1968

年这一称谓消失，女性正式并入"黑豹党"（Spencer 2008）。女性被力量与美德的形象所吸引，而"党内领导者那种直面冲突的阳刚作风"有时令她们疏离（Josephs 2008: 410）。此外，党内女性成员通常比男性接受过更正规的教育（Williams 2012: 40, Spencer 2008: 97）。到1970年，女性已成为黑豹党的主体力量（Nelson 2015, Josephs 2008），而休伊·牛顿正积极倡导与女权运动及同性恋运动建立联盟。

黑豹党中的性别问题

理论上，该党实现了性别平等，其党报将女性称为"同志"和"战士"（Bloom and Martin 2016, Josephs 2008, McBean 2014）。这种平等尝试在其所处时代尤为引人注目。而由法拉罕领导的美国组织和伊斯兰民族等类似团体，则未给予女性同等地位。鲍比·西尔在自传中阐述黑豹党的立场："我们认为，姐妹也是革命者，她必须像我们一样学会自卫。像我们一样学会射击。因为体制内的猪猡根本不在乎她是姐妹，他们同样会残暴对待她」（1996: 398）。黑豹党认为男女皆可能遭受警察暴力，因此必须在革命立场上实现平等（Josephs 2008, Seale 1978: 178）。

一些女性黑豹党成员表示并未感到被排斥（Jennings 2001），例如凯瑟琳·尼尔·克利弗曾说："有人会问'女性在黑豹党中扮演什么角色？'我向来不喜欢这类问题。我会简短回答：' '和男性一样'。我会解释：我们都是革命者"（Cleaver 1999: 232）。1969年，六位匿名黑豹党女性接受了题为《黑豹姐妹论妇女解放》的小册子采访。受访者坦言组织曾存在沙文主义倾向，但强调"姐妹们必须像兄弟们那样拿起武器"。埃里卡·哈金斯在丈夫遇刺、自身遭警方追捕后展现的坚韧与领导力，被男女成员共同视为“改变党内性别动态的关键” —— 她彻底重塑了黑豹男性对女性成员的认知（Spencer 2008）。此外，该组织将越战中抗争的越南女性奉为典范。"越南女性实际上扮演着另一半的角色 —— 既非弱势半边，亦非强势半边，而是越南男性不可或缺的另一半"（Bukhari-Alston 1969）。该组织政策规定男女共同承担日常事务与家务，包括烹饪、接听电话、清洁及照看孩童（Nelson 2015）。

其他记录揭示了该组织内部性别问题的矛盾性与复杂性。尽管性别歧视被视为问题，但种族主义和资本主义问题的优先级明显高于性别歧

视。性别政策的实施取决于各支部所在地区（Bloom and Martin 2016: 97）。黑豹党唯一的女性主席伊莱恩·布朗指出，多个分部的兄弟们认为"像我们这样'聪明的婊子'......必须被封口"（Brown 1993: 192）。安吉拉·戴维斯和阿萨塔·沙库尔同样提及该组织的"男性化特征"（Davis 1974: 161）及"男子气概崇拜"（Shakur 2001: 223）。在自传《阿萨塔》中，沙库尔坦言："我们许多女性为在黑豹党中生存，不得不效仿那种男子气概的风格。说出 '兄弟，我认为...我们该这样那样' 类似的话，实在是太难了。" 要想被人听见，就必须说'听着，混蛋'。你得培养出这种傲慢的男子气概才能发声 ...... 我们每天都在黑豹党内部为争取尊重而斗争"（2001:422）。即便像弗雷德·汉普顿这样的领袖 —— 他以倡导党内女性平等著称 —— 也曾宣称"洗碗扫地是'女人的活儿'"（Williams 2012: 42）。

运动初期，随着男性领袖相继被捕或遇害，众多女性开始担纲领导重任。西尔、牛顿和埃尔德里奇·克莱弗均面临警方的严重指控。为逃避起诉，克莱弗与牛顿分别逃往古巴（克莱弗后又转赴阿尔及利亚）。凯瑟琳·克莱弗成为中央委员会首位女性成员，并逐渐成为该党广为人知的公众形象（Spencer 2008）。后来，在牛顿流亡后，伊莱恩·布朗成为黑豹党唯一的女性主席，并以提拔更多女性担任领导职务而闻名（Brown 1993: 362）。在地方层面，女性的作用尤为重要，却常常被低估（Phillips 2014）。"无论我在费城、布朗克斯还是加州伯克利，都服从于一位女性黑豹领导人 —— 她管理得井井有条，且高效"（Abu-Jamal 2004: 180）。部分男性成员认为该党正变得"软弱"，女性正在"侵蚀黑人男性气概"（Brown 1993: 357）。

[image]

黑豹党中的性关系

党内成员间的性关系十分普遍。身为黑豹党成员具有亚文化资本，"赋予他们巨大的性吸引力"（Nelson 2015）。该组织有时会利用有吸引力的女性成员招募新成员（Bloom and Martin 2016: 96）。某些情况下，女性被告知与黑豹男性发生性关系是她们的“义务”（Lumsden 2009: 910）。鲍比·西尔在自传《孤独的愤怒》中回忆，该组织曾因一名女性拒绝与党内成员发生性关系而将其开除，并指出这种压力是错误的："实际上她们别无选择"（1978: 117）。有记录显示，弗雷德·汉普顿等领导人曾公开谴责强奸行为（Williams 2012: 43）。

但在其他情况下，党内成员将性视为一种奖赏。伊莱恩·布朗在其自传《权力的滋味》中回忆了鲍比·西尔与玛莎姐妹关于女性角色的对话："姐妹必须学会射击和烹饪，随时准备支援兄弟们。姐妹们必须熟记十点纲领和行动计划。" 鲍比追问："还有呢？" "当兄弟在执行任务时，姐妹必须献出肉体；当兄弟不在时，则必须守护住肉体。因为姐妹们掌握着阴道权力"（1993:189）。同样，埃尔德里奇·克利弗主张"阴道权力"可作为"对男性政治行为的奖励"（Spencer 2008:104）。值得注意的是，在探讨性行为同意权时，埃尔德里奇·克利弗在加入黑豹党前曾因强奸罪被定罪。该党曾推荐成员阅读克利弗著作《冰封的灵魂》，书中他坦言过去认为"强奸是起义行为……我最初在贫民窟的黑人女孩身上练习……自认足够老练后，便越过铁轨寻找白人猎物"（33）。后文他阐述了对种族问题的认知转变，并谴责了强奸行为。

该党政策反对一夫一妻制，旨在"避免因琐碎嫉妒和无谓争吵破坏未来争取自由斗争的整体目标与宗旨"（Seale 1978: 187）。对部分人而言，这意味着男性可与党外女性发生性关系，而女性则不可（Alameen-Shavers 2017）。但另一些观点指出"女性选择伴侣的自由度与男性相当，许多人能够且确实拒绝过"（Abu-Jamal 2004: 182）。在缺乏性别与性关系领域更广泛的文化变革时，非一夫一妻制往往更有利于男性而非女性。

若女性拒绝男性性邀约或抗拒非一夫一妻制，部分人会被指控缺乏对革命事业的忠诚。女性可能被"排除"在组织活动和信息流通之外（Spencer 2008: 104），被迫接受"荒谬指令"（Jennings 2001: 150），被冠以"反革命分子"（Seale 1996: 397）或"资产阶级"（Josephs 2008: 425）。正如黑豹党成员里贾纳·詹宁斯所言："白天在街头抗争压迫、协调社区项目，晚上还要把黑豹兄弟赶下床，这种生活令人不堪重负"（Josephs 2008: 425）。尽管官方党规明确提出"不得侵犯女性"，但中央委员会却站在骚扰者一边，认为"她坚持禁欲的态度既愚蠢又反动"（Jennings 2001: 151）。

内部争端和自我批判

联邦调查局的秘密反情报计划加剧了该党的内部矛盾。反情报计划（**COINTELPRO**）通过卧底特工渗透活动团体，采用不受约束的监控手段和策略性破坏行动，诋毁成员及其事业（Churchill and Wall，

2001）。行动目标涵盖美洲印第安人运动组织、民主社会学生会及其他黑人民族主义、女权主义、社会主义和反战团体，但联邦调查局最关注的对象是黑豹党。该计划的终极目标在于收集情报、煽动参与者内部分裂、诱使团体实施激进非法行为以致被捕，从而瓦解整个运动。

无论冲突源于何处，黑豹党内部的纠纷始终缺乏统一的解决机制。黑豹党成员埃默里·道格拉斯认为该组织拥有"问责体系"，并设有"处理各类情况的机制"（Spencer 2008: 101）。同样，鲍比·西尔也承认该组织"制定了明确规则"，但他坦言"遏制此类事件实属不易"（1996:402）。某些情况下，黑豹党成员会采用肢体暴力实施纪律处分（Williams 2012, Brown 1993）。当休伊·牛顿从国外归国后重新担任主席，批准对黑豹党学校管理员雷吉娜·戴维斯实施惩罚时，伊莱恩·布朗最终脱离了该组织。一名男性黑豹党成员因被戴维斯训斥而对其实施暴力袭击，导致其下颌骨骨折。其他情况下，黑豹党会暂停或驱逐涉事成员党籍（Seale 1996），例如某男性成员强奸年轻女成员事件（Cleaver 1999: 235），或密尔沃基支部全体男性成员虐待女性的丑闻曝光后（Williams 2012: 43）。部分成员如雷吉娜·詹宁斯和伊莱恩·布朗指出，当时"根本无法质疑"决策（Jennings 2001: 150），“我们的司法系统基本上是随走随编的”（Brown 1993: 275）。

黑豹党常将人际问题视为其职责范围之外。尽管鲍比·西尔曾数次承认需要通过政策介入，但他仍将男女成员间的感情纠纷称为"琐碎问题"（1996: 401）。当领导者本身就是沙文主义同情者、甚或就是施暴者时，这种态度尤为突出（Alameen-Shavers 2017: 114）。众所周知，埃尔德里奇·克利弗曾殴打妻子凯瑟琳（Spencer 2008:100），休伊·牛顿则犯下性侵罪行（Nelson 2015）并殴打伊莱恩·布朗。当布朗的另一位情人施暴时，牛顿回应道："这或许违反了党规，但绝对不属于党务范畴。"他最后总结道： "总之，我本就不该和这种'丑陋的黑鬼'上床，" 他总结道（Brown 1993: 313）。其他领导层成员则告诉她"此事过于私人化不宜由党来裁决"，并称"她'活该'"（McBean 2014）。

党内有人认为，女性只需挺身而出，拒绝容忍他人恶劣对待。黑豹党成员布伦达·哈里斯指出："如果女性缺乏自我保护的能力，就必然会面临遭受性剥削的危险"（Williams 2012: 41）。琼·格雷同样指出："如果你是那种默许某些行为发生的女性，那么这些事情就会发生

在你身上……"（Williams 2012: 41）。黑豹党将变革的责任与动力交到女性手中。杰基·哈珀告诫黑豹女性要"向男性表明她们'是认真的'...以赢得尊重"（Josephs 2008: 422）。尽管黑豹党女性"并非娇弱怯懦之辈"（Abu-Jamal 2004: 180），但部分成员仍因这种权力动态退出组织或转投其他团体（Davis 1974, McBean 2014）。

无论评价褒贬，黑豹党在其所处的时代背景下，对女性持的态度是自由派的，为女性提供了自主行动与批判的空间。该组织调整其预示性政治策略，聚焦于自我教育和挑战传统思维模式。即便实践中未必完全贯彻，该组织在理论层面至少认可了如今所称的交叉性理论，在种族议题中兼顾阶级、性别及其他关切领域。本节提及的众多黑豹女性事迹，源于作者们希望"唤醒年轻的活动家兄弟姐妹们认识历史 ... 或许往昔的错误不会重演于未来"（Jennings 2001: 147）。

[image]

争取民主社会学生组织（SDS）和地下气象组织（WUO）

民主社会学生会（SDS）是1960年成立的校园学生运动组织。该团体源于工业民主学生联盟，以参与式民主形式运作，深受同期学生非暴力协调委员会（SNCC）及后来的黑豹党影响（Flacks 2013: 1284）。

1962年，SDS通过《休伦港宣言》作为组织纲领。这份由汤姆·海登起草的文件批判政府、种族与经济分层，倡导非暴力理念，并呼吁"反抗冷漠的生存状态"（Hayden 2005: 4）。

该组织规模迅速扩张，从1960年的约1万名成员发展到1969年拥有10万名正式成员，非正式成员数量更为庞大（Barber 2010, Cornell 2016）。这种增长部分源于越南战争征兵政策的实施、性观念的转变，以及围绕毒品与音乐兴起的蓬勃青年文化。杰克·温伯格那句著名的"别相信任何超过**30**岁的人"，生动地体现了这种文化断裂（Galloway 1990）。在此期间，早期老成员和新晋年轻成员之间矛盾不断。尽管《休伦港宣言》在某种程度上统一了共同意识形态，但在日益激烈的斗争环境中，关于马克思主义与社会主义的细枝末节仍

持续引发紧张对立。

1968年，由于认为既有策略无效且存在意识形态分歧，SDS分裂为两个组织：革命青年运动（RYM）自诩为受压迫者的代言人并主张革命行动；工人学生联盟（WSA）与进步劳工组织（PL）则植根于毛主义，专注于劳工议题（Cornell 2016）。SDS-WSA分支作为全国性高校组织延续至1970年代中期，成员大幅减少，主要开展非暴力行动与抗议活动。RYM大部分成员解散，残余力量（主要为SDS内部领导层）重组为地下气象组织/气象员（WUO），该组织持续实施更具暴力性与戏剧性的行动直至1980年代初（Glass 2013: 1394）。

性别问题在SDS（学生非暴力协调委员会）乃至后来的WUO（地下气象员）中始终是持续斗争的焦点。前文提及的凯西·海登与金曾向SDS女性成员发送题为《性与种姓：一份备忘录》的文件。一个月后，受此文启发的女性团体在SDS全国代表大会上集体退场。她们组建了"妇女核心小组"，但最终仅促成一项"极其温和的决议"，确认女性参与权与成员资格（Barber 2010: 106）。1967年全国大会上该议题再度浮现，但成员们将其纳入更广泛的平等与反帝国主义论述中，从而"将应对性别歧视的责任推给了女性，而非整个SDS组织"（Gilbert 2000：60）。这种分裂部分源于SDS的抗争活动主要针对越战及青年征兵制度。成员苏珊·斯特恩回忆道："女性几乎被系统性地排斥在核心决策之外...但我们确实开始迫使男性领导层与我们共同承担激进运动的重担"（Stern 2007：50）。尽管我阅读的大多数男女亲历者叙述都承认不同程度的性别问题，但参与六十年代初至中期的运动、并在与SNCC工作相似的分支中活动的女性 —— 如凯西·海登和卡罗尔·格拉斯曼 —— 都表示她们作为SDS成员感受到被尊重与赋权（Garvy 2000）。

尽管SDS承认性别歧视是个问题，但领导层却阻止女性加入女权运动或组建全女性工作组。SDS/WUO认为女性解放将在推翻资本主义“后”实现（Higuchi 2013）。许多成员将性别歧视视为其他男性造成的现象，认为这是组织外部存在的抽象范畴。SDS组织间事务秘书、WUO主要组织者伯纳丁·多恩并没有将此问题视为结构性问题，她主张女性必须改变自身，"停止像女人那样行事"（Barber 2010: 137）。SDS领导层认为女权运动是"自我放纵"的"心理治疗"（Barber 2010: 140）。

领导层架构

与同时代其他新左派运动相似，SDS/WUO存在明显的性别化分工。该组织中的女性成员如简·亚当斯、玛吉·皮尔西和贝蒂·丘宁指出，女性承担了大部分日常且隐形的劳动，包括冲泡咖啡、打字、烹饪和清洁。男性则垄断决策过程，负责理论构建与高谈阔论，成为"可见且受尊敬的存在"（Evans 1980: 177）。SDS/WUO领导人马克·拉德曾指出："女性是基层执行者和打字员"，而"男性才是理论家和演说家"（Rudd 2010: 122）。尽管有人将女性角色扩展至"亲密关系（或仅指'亲热一下'）…… 唯当涉及站在街垒上抗争或入狱服刑时……女性才被视为平等者"（Browder 2007: xxii）。

看似矛盾的是，SDS争取平等的斗争中，大多数领导者都来自最负盛名且财力雄厚的大学（Barber 2010）。SDS/WUO选举产生的全国领导层几乎清一色是男性（Garvy 2000）。在会议中，男性通常表现出竞争性和攻击性。苏珊·斯特恩指出："会议中说话最响亮、最快的人总能赢得辩论"（Stern 2007: 43）。早期领袖、《休伦港宣言》作者汤姆·海登曾坦言该组织"充斥着强势男性自负"，他本人尤其 "仗势欺人且 …… 对批评置若罔闻"（Miller 1994: 271）。

女性在争取领导职位甚至参与SDS会议方面都受到限制。苏珊·斯特恩指出，在会议上男性领导者根本不听女性发言。"奥格尔斯比会若有所思地微笑，克隆斯基会拨弄头发或手指，拉德会在房间里踱步并敲打物品，其他明白事理的女性则显得尴尬难堪"（Stern 2007:43）。1960年代初，女性在SDS的经济研究与行动项目（ERAP）中稍有施展空间，但全国层面仍由男性主导（Barber 2010, Evans 1980, Cornell 2016）。1967年玛丽莲·巴克在SDS全国大会演讲时，"男性哄笑吹口哨 …… 投掷纸飞机 …… 高喊'我用我的鸡巴解放你'之类的'妙语'"（Gilbert 2010：58）。另一次在尼克松就职典礼的SDS示威活动中，当女性发言时，男性竟发出"脱掉衣服！" 的猥亵口号。"干她！" "把她赶下台！在后巷强奸她！"（Barber 2010: 10）。SDS/WUO领袖比尔·艾尔斯在其缺乏反思的自传中写道："我嘲讽道：女人当家房倒屋塌(Chicks in charge)"（2009: 104）。

少数担任领导职务的女性通常参与阳刚文化，且不挑战男性领导者的议程（Barber 2010, Berger 2005）。这些女性往往"隶属于异性恋领导伴侣 …… 渴望领导地位的女性会感受到某种压力"（Gilbert 2010:

187）。最著名的女性领袖是伯纳丁·多恩，她当选为 SDS 的跨组织秘书，后来领导了革命青年运动（RYM）的解散和工人联合组织（WUO）的成立。当时的FBI 局长埃德加·胡佛给她起了个绰号叫"左疯子的激情之花"，许多自传和历史记载都描述了她的魅力和性感（Rudd 2010, Ayers 2009, Stern 2007）。多恩贬低女权运动，鼓吹暴力抗争，并发出驱逐保罗·莱文斯顿出SDS的著名号召。有人认为多恩"美得令人难以正视"，而她时常以敞开衬衫至肚脐的装束主持会议，胸前别着 "舔阴很酷，口交很爽" 的徽章，更强化了这种魅力（Burrough 2016: 41）。

该组织的过度阳刚气质与内部竞争，折射出其从非暴力转向暴动手段的转变。SDS/WUO领导人热衷于相互攀比的言论。"你必须更加激进些 …… 更愿意冒险来证明自己"（Klatch 2004: 495）。到1969年，SDS发起"将战争带回家"运动，鼓动成员获取武器采取激进行动。该组织常用口号是"越南妇女都持枪！"，并开始将言论转化为武装斗争（Rudd 2010: 166）。这场战术转变在1969年10月由"气象员"组织策划的"愤怒日"行动中达到顶峰。为宣传活动，SDS/WUO女性成员实施了"越狱"行动 —— 一种戏剧化的抗议形式：活动家冲进校园扰乱课堂，向学生分发传单（Berger 2005: 101）。参与者预期数千人汇聚，实际仅200人到场。值得注意的是，"愤怒日"中另设独立的女性行动。但无论是女性行动还是整个"愤怒日"，均未取得显著成效。当地黑豹党领袖弗雷德·汉普顿将SDS和"愤怒日"运动斥为"无政府主义、冒险主义、沙文主义、个人主义、自虐主义和卡斯特式的（意指像卡斯特将军那样鲁莽送死）"（Rudd 2010: 173）。当"武器组织"实现自治后，该团体开始实施炸弹袭击，通常事先通告以避免人员伤亡（Ellis 1996: 111）。

[image]

关系与性

在SDS/WUO中，性关系是核心议题，能激发参与热情（Stern 2007）。在《利维坦》报刊中，活动家们援引了"鲁德和JJ实践的'组织'方式：'通过性行为组建团队'"（引自Barber 2010: 197）。如果女性拒绝发生性关系，则被视为保守拘谨，不具革命精神（Evans 1980, Klatch 2004）。SDS/WUO成员、后成为黑人解放军（BLA）合作者的大卫·吉尔伯特在其自传中指出："男性将'自由恋爱'作为工具，使女性在性方面可供利用，而非作为让爱与平等蓬勃发展的契机"（Gilbert 2010: 60）。女性在关系中遭遇的问题，最终被归咎

于"她们自身的缺陷"（Gilbert 2010: 52）。

SDS/WUO的领导人经常在美国各地奔波，他们从不断变化的性道德观念中获益。马克·拉德回忆道："不可避免地，女性会主动示好，或者是我主动接近她们 …… 我把那些一夜情视为自己微不足道的明星光环带来的福利"（Rudd 2010: 122）。女性成员为争夺关注而产生的紧张关系日益加剧，她们渴望"接近权力核心"，而领导者有时会利用这种情况谋取私利，获取金钱、交通工具及其他资源（Rudd 2010: 166）。与拉德不同，艾尔斯至今仍对自身特权与权力差异浑然不觉。他坦言："每次与女性交往时，'何时或能否发生关系'的念头总在脑海潜伏 …… 最美妙的是，我们总会顺势而为，至少亲热一次，事后再处理后续"（Ayers 2009: 105）。苏珊·斯特恩评价艾尔斯时说："他身上有种令我无法忍受的特质，仿佛认定全世界女性都渴望与他发生关系……这种心态在SDS男性中很普遍"（Stern 2007: 76）。凯西·威尔克森在评论艾尔斯自传时反驳道："女性承受的性同意压力极其巨大"，并指出"艾尔斯至今毫无反思，尤其面对女性多次试图阐明……当时经历的种种感受时，这种态度令人费解"（Wilkerson 2001）。

SDS/WUO将个人与政治融入预示性政治的实践中，使性行为成为政治行为。活动家们将性等同于“解放”，认为群交能创造"爱侣军团"（Ayers 2009: 142）。但多数关于SDS/WUO集体性行为的记录都显得冷漠而令人不快（Rudd 2010, Burrough 2016）。尽管存在恐同现象，男性仍面临与其他男性发生关系、女性则需与其他女性发生关系的压力（Gilbert 2010: 140）。这并非LGBTQ运动的组成部分，其核心更在于反抗压迫。同性恋的SDS/WUO成员仍处于隐秘状态（Hayden 2005, Rudd 2010）。

1969年夏天，SDS/WUO通过"打破一夫一妻制"倡议规范了性行为准则。大卫·吉尔伯特在其自传中阐释了该政策的双重逻辑：既批判被视为"男性至上主义核心制度"的传统核心家庭结构，又防止伴侣间的情感纽带超越群体忠诚（Gilbert 2010: 125）。值得注意的是，多恩与其伴侣杰夫·琼斯得以豁免，但其他一夫一妻制伴侣则被刻意拆散。领导层宣称女性尤其能从这些政策中获益，必须"抛弃男友、子女、父母、学业 —— 任何阻碍你投身革命的事物"（Stern 2007: 76），即便违背其意愿亦然（Wilkerson 2010: 269）。

这些关系形式的政策与压力带来了诸多后果。"滥交"导致性传播感染大行其道。"淋病、盆腔炎、阴虱以及我们称作'气象员脏病'的非特异性生殖器感染在成员中间流行。"（Rudd 2010: 166）。强迫伴侣与他人发生性关系导致同意权存疑。斯特恩在自传中描述鲁德胁迫其友人发生关系的情景 —— 友人反复表示"不要"、"我不想"、"求你别这样"，而鲁德据称回应道："集体利益高于一切……"（Stern 2007: 176）。其他领导层明知特里·罗宾斯对伴侣实施身体虐待却保持沉默。1969年期间，因"打破一夫一妻制"理念及WUO内部人际关系问题，许多成员相继离开该组织。

问题、批评与自我批评

受毛泽东“红宝书”启发，SDS 通过批评/自我批评会议实现成员间的相互监督（Miller 1994, Rudd 2010）。通常由多人聚会，将批评聚焦于某位成员身上。批评/自我批评会议可随时召开，持续长达6小时，且往往充满激烈攻讦（Berger 2005: 105）。从功能上看，这是提供反馈、解决个人问题并强化成员心理韧性的途径。凯茜·威尔克森指出，这是女性集体对抗男性的少数有效方式之一（Wilkerson 2010: 288）。会议始终强调个人服从集体原则。大卫·吉尔伯特认为这类会议大多糟糕透顶，但他曾经历过一次积极的建设性的会议。"尽管女性们严厉谴责我那令人无法忍受的轻率态度，以及我如何伤害深爱我的女性，但会议也传递出希望 —— 我值得她们付出努力，即便被厚重的男性沙文主义包裹并玷污，我体内仍潜藏着革命者特质"（Gilbert 2010: 55）。另一案例中，同性恋SDS成员迈克尔·诺维克因"否认自己渴望与众多女性发生性关系"而遭男性成员批评（Berger 2005: 105）。

除批评会议外，组织内部几乎不存在问责机制。某些活动中，该团体甚至组建了专属"安全部队"以避免内部肢体冲突（Stern 2007: 65）。领导层将信息和"更具声望的工作"限制在少数人手中，被视为软弱者可能导致晋升受限（Wilkerson 2010: 317）。SDS/WUO成员害怕被边缘化，因此"格外重视与掌权者建立特殊特权关系"（Wilkerson 2010: 360）。对领导层的批评不受重视（Berger 2005: 290），且"领导者刻意压制内部冲突"（Wilkerson 2010: 312）。由于SDS/WUO成员过度强调行动实践，"无人再关注组织内部的动态演变"（Wilkerson 2010: 297）。

SDS/WUO指责那些离开组织参与同性恋运动的女性具有"分裂性"（Gilbert 2010: 59），并瓦解了试图在SDS/WUO内部组建的女性团体（Berger 2005: 292）。SDS/WUO的男性成员"要求我们不断宣誓效忠于他们，而非独立的女性运动。SDS内部的女性必须每隔五分钟就在每次讨论女性议题时谴责分离主义，否则将被禁止继续参与"（Grele 1985）。

该组织向更激进观点的转变与其运动规模的扩张形成矛盾。尽管多恩在古巴曾建议保持组织对大众的开放性，但艾尔斯和拉德却"胁迫伯纳丁顺应整个夏天形成的'将战争带回家'路线"（Rudd 2010:167）。政府虽未像对付黑豹党那样大规模动用反情报计划打击SDS/QUO，但该计划仍对组织产生了影响。成员们开始自我神话化，例如比尔·艾尔斯宣称"我本就是个叛逆者，如今将蜕变为自由斗士"（Ayers 2009: 71）。鲁德在自传中反思道："当时我并未意识到，我们无意间复制了所有封闭式邪教的运作模式：隔离、剥夺睡眠、强迫成员进行任意的忠诚行为，甚至以性仪式作为凝聚手段"（Rudd 2010: 162）。

尽管秉持激进理念，SDS/WUO在性别与种族问题上仍面临诸多内部矛盾。马克·拉德在其自传结尾处描述了四十年后的活动家会议，他坦言女性"承担了绝大部分繁重工作"，而非洲裔学生未获应有认可（Rudd 2010: 319）。在哥伦比亚大学占领期间担任罢工协调委员会唯一女性成员的鲁斯蒂·艾森伯格在会上指出："作为女性、研究生、哥伦比亚校园的新人以及异议者的发言人，我在罢工协调委员会中备受排挤。当时那群年轻男性的男子气概和轻蔑态度令我深受伤害且震惊。"如今回想起来，唯一例外的是大卫·吉尔伯特 —— 尽管我们存在政治分歧，他那份敏锐体贴的品格令我至今难忘。"吉尔伯特因参与1981年著名的布林克斯抢劫案，被判终身监禁（Rudd 2010: 320）。最终，SDS/WUO的女性成员并未获得比先前社会运动中女性更好的处境。

社会运动中的模式

在SNCC、黑豹党以及SDS/WUO 中，组织架构与人际关系模式呈现出相似特征。这三个团体虽然都推行性别平等政策，却普遍存在将女性局限于传统角色（如记录会议和打扫卫生）的问题。SNCC与黑豹党的全国领导层以男性为主，但女性在地方层面掌握实权。相较而

言，SDS/WUO的女性成员在争取领导职位方面面临最大阻力。

正如本章开篇引用的阿萨塔·沙库尔所言，参与这些社会运动的人士 —— 尤其是黑豹党气象员组织 —— 事后都批评了运动中缺乏问责制和申诉框架的问题。这些活动家的知识与经验并不是总能传承给年轻一代的，社会运动往往难以吸取历史教训。活动家们常常复制了性别、种族和阶级层面的权力动态。虽然SNCC、黑豹党及SDS/WUO对现代社会运动产生了深远影响，但组织者至今仍未解决人际关系动态中存在的问题。

[image]

第四章 组织、性与关系

在当代社会运动中，参与行动主义似乎意味着具备特定的道德品格。理所当然地，行动者 —— 尤其是参与女性主义或酷儿运动的人 —— 本应当更深刻地认识性别歧视与异性恋霸权，并据此调整自身行为。同为行动者的同伴们因投身于更宏大的政治斗争而被视为“具有美德”，这似乎与文化中对性别歧视者的刻板印象相悖。尽管行动者个体的惯习可能植根于既有的社会不平等，但行动领域的规则要求挑战这些倾向，并创造更平等的社会实践。

尽管存在隐含的政治诉求，主流文化的压迫却往往被延续下来了，而平等主义政治理念并不总能在社会互动中得到体现。正如一位自认女性身份的虐待关系幸存者所言："社会权力与政治正义感经常能蒙蔽真相"（Wrekk 2007）。激进主义文化可被视为"充斥着'白人男性特权异性恋'氛围"，其核心在于优先考量表象上的真实性、影响力、有效性及激进程度（Quarrel 2013: 90）。正如"莫莉·托夫"在《社会排毒》中所言："一旦男性给自己贴上'革命者'的标签，他们便不再是问题的一部分 —— 尽管他们确实就是问题所在"（2007）。

过度阳刚的行为似乎与亚文化中反对性别本质化的趋势相冲突。激进左翼亚文化在意识形态上批判男性/女性二元对立，反对将出生时指定的生理性别与性别认同混为一谈。当然存在例外，例如排斥跨性别的激进女权主义者（TERFs）。但总体而言，该亚文化的活动家们更倾向于拥抱复杂而细腻的身份认同，如酷儿性别和非二元性别。一位

自认性别酷儿的受访者表达了担忧：性别解构可能被滥用来否认女性及非二元性别者面临的结构性不平等 —— 即反对聚焦性别不平等的论调，认为我们应当致力于消除性别概念本身。

然而，活动家们仍在围绕阳刚气质问题持续抗争。文化中戏谑地使用了两个合成词："大男子主义无政府状态"（manarchy）和"兄弟主义"（broism）或者"兄弟社会主义"（brocialism）。这些术语指代某些活动家展现的极端阳刚行为与态度。底层的活动家文化往往强调攻击性、竞争性、好战性、纯粹性和自以为是等价值观。费城一群匿名无政府女权主义者创作了名为《你是“manarchy”吗？》的问卷，该问卷被广泛复制传播，收录于《打破枷锁》等独立刊物中。问卷细分为多个板块，包含若干"行动主义问题"，例如第12题："你在组织工作中承担'脏活'或'苦差事'吗？（例如：烹饪、清洁、场地布置、善后整理、电话联络、邮件列表管理、会议记录、后勤支持、邮件寄送、托儿服务？）" 以及"性/情感关系问题"，如第27题："如果女友指责你父权行为或试图在关系中解决父权问题，你会分手还是出轨另寻能容忍你行为的女性？"。受访者普遍知晓"manarchy"这个词的含义。有受访者特别指出，虽然该标签从未针对自身使用，但他们曾称呼他人为 manarchy。

> 未经审视的有毒男性气质 …… 就像一个万能模板，能套上任何面具。它既能披上兄弟会成员的面具，也能戴上黑群起义者的面具，但本质上始终在演绎相同的动态机制 …… 我见过许多人仅听到这个词就极度抵触，这本身就很有深意。这恰恰说明它如同带电的导线，是男性群体最敏感的神经末梢 —— 他们根本不愿削弱自身权力，更不愿挑战父权制根深蒂固的权力关系。" —— 亚历山德拉，12:10

尽管这种美学可能属于亚文化特有的范畴，但其背后的性别与男性气质观念与主流社会并无二致。

如同许多其他亚文化群体，阳刚特质与行为被赋予文化资本的价值。当这些特质“被视为”更具原初激进性的象征而获得正当性时，便会促使女性效仿。在《首张7寸唱片更胜一筹》中，妮娅·金回忆起在演出现场见 到一位身着女性化服饰的女孩时，曾疑惑"她究竟是谁的女友？难道我们不都清楚朋克圈是男人的游戏，必须比男人更像男人才

能胜出吗？"

确实存在一些围绕解决男子气概和性别问题而组织起来的男性社会运动团体，尽管部分男性批评这些团体“过分强调社会化过程中的个人困境，而较少审视其当代实践”（Ex Masculus 2014, Men Against 1996, Rae 2008, Kooky）。这种缺乏反思性的问题或许超越了性别动态范畴。妮娅·金曾批判整个亚文化圈缺乏自我审视：

[image]

"我们为移民权利组织活动，却不认识任何移民，甚至没有有色人种朋友。

我们举办“同意权”工作坊，却对社区成员举报朋克施暴者毫无应对之策。

我们高喊阶级冲突口号，却以为翻垃圾桶和偷窃就能“洗刷阶级特权”（事实并非如此）。

我们是口是心非的伪君子，只愿谈论表面，

却回避那些令人不安却能促成真正变革的深层问题。"（2012年）

在本章中，我探讨了性别歧视与父权制如何在激进左翼亚文化中显现。尽管这些动态相互交织，我仍将本章分为"组织活动中的性别"与"性行为中的性别"两部分。这种划分方式与第三章所述的先前社会运动中的区分相呼应。我认为将这些范畴视为独立存在有助于厘清问题本质，同时揭示活动家们为解决这些问题所采用的不同策略。通过这两个部分，我将揭示亚文化中的社会资本与文化资本如何助长问题的延续。本章结尾将回顾围绕安全文化中的性别歧视问题及运动优先事项的论辩。

[image]

组织中的性别问题

领导力

构成亚文化或"社群"的团体拥有内部架构，这种架构将流行的激进意识形态与能动性转化为常规的社群实践。团体采用去等级化的/或水平式的关系结构，成员间不存在权威或等级差异。正如我们已停用的无政府主义社区空间宣传册所述："这里没有领导者，不存在等级制度。所有志愿者或参与空间活动的人员均享有平等的决策权"（123 Community Space）。

尽管团体理论上运作于等级制度之外，但“领导者”仍不可避免地涌现。社区内部有人认为领导岗位的构成反映了性别歧视，其中绝大多数是顺性别男性。正如社区内流传的一本杂志所言："无结构的'去中心化'组织往往存在事实上的领导者，而且通常是男性，他们凭借意志力与经验强行推行己见"（Said the Pot）。缺乏结构意味着"无法平衡特权群体与受压迫群体"（Beallor 2001）。这种水平式组织模式的困境，早在35年前乔·弗里曼在《无结构的暴政》中就已指出：在社会其他领域享有特权的人，往往在激进团体中延续其支配地位。

[image]

提醒注意，这里所言之“领导人”事实上是“指挥官”，而不是“成核点”，我们需要的是后者而不是前者。延伸：https://www.patreon.com/posts/wei-shi-yao-bao-85963903

多年来我作为活动家参加过无数次会议，其间没有哪个团体任命过正式的“领导人”，但少数团体存在非正式领袖。某次男女混合团体召开周例会时，议程上有项重要议题。该团体的非正式领袖 —— 一位男性活动家未能出席会议，在场成员（多为女性）以需要更多时间审议为由，将议题推迟至下周讨论。次周他再度缺席，议程事项再次被搁置。尽管未被明言或确认，但成员们显然不愿在领袖缺席的情况下做出关键决策。

除特定性别的女性团体外，我领导的"要食物不要炸弹"组织是个例外。我本无意主导各项项目，也未担任正式职务，但实际上却成为了团队“核心”。原因很可能是该组织以烹饪食物为中心。早期便显而易见，我是成员中烹饪经验最丰富的人，尤其擅长使用全食物原料制作

纯素料理。鉴于美国女性烹饪时间是男性的两倍以上（劳工统计局2013年的数据），我在厨房的熟练程度恰恰符合传统性别角色定位。当组织转型为减少烹饪、增加食品分发时，非正式领导权便转移给了拥有车辆的男性成员。

[image]

被视为领导者可以意味着拥有社交资本。

一位受访者将"圈子"中的社交资本定义为"源于各类资源 —— 无论是智力的还是物质资源，以及推动事情发生的能力。

如召集会议时是否有人响应？发起特定活动时是否获得全员配合？"（11:15 Lee）

拥有魅力与人脉网络，等同于具备高效达成目标、凝聚人心的能力。

会议与共识

虽然没有等级制度，但团体仍有秩序或框架。参与者承担不同角色：一人自愿担任会议主持人或协调员，负责优先排序议程事项、大声宣读议题、严格把控时间、引导讨论并管理共识形成过程。另一人负责记录，通常以打字形式整理后发布至在线邮件组或论坛。如果团队规模较大，可能增设"氛围观察员"，专注于感知团队内部的紧张情绪与情感波动。在固定成员的团队中，成员们会认真分配职责，每周轮换承担这些角色。

决策需要达成共识。与多数决不同，群体必须认可每个人的意见并达成一致。每位成员必须明确表态赞成、反对或弃权。虽然共识通常通过口头表达达成，但在更具女性主义和酷儿倾向的群体中，曾采用"闪亮手指" —— 即向上摆动的指尖作为同意信号。后来，占领华尔街运动的会议也沿用了"闪亮手指"或"女性主义爵士手势"（Johnston 2015）。

如果有人不同意，他们会说明不同意的原因，或提出任何可能改变或

澄清其判断的问题。如果多人有问题和评论，他们会进入“发言队列”（stack），这是根据人们示意想发言的顺序确定的队列。有顾虑的成员随后提问，讨论继续进行，直到所有人同意。理想情况下，共识意味着个人之间没有怨恨、结盟或疏离。任何人都不应该做或参与他们不同意的事情，从而创造一个相互欣赏和赋权的环境。

然而这种方法可能变得艰巨，权力博弈也可能随之浮现。有时会议中会出现"搁置"议题的情况—— 那些看似无休止的分歧会被移至下周议程。主持人有权决定最终议程的构成及各议题的分配时长。当社会资本或文化资本更丰厚者达成共识时，与会者可能面临按特定方式回应的压力，至少需避免参与决策。一位受访者在谈及组织工作时，就指出了这些问题。

> 我也曾对参与集体决策过程充满热情，憧憬着人人拥有某种程度的平等决策权 …… 我确实开始参与集体决策，努力践行这些理想，却未能更深入地理解内化的压迫如何在群体中显现 —— 无论是对他人，还是对我自己。尽管我们总说 …… 是的，每个人都是平等参与讨论的，但如不审视 …… 在群体动态乃至更广阔的社会中，每个人如何掌握权力或缺乏权力，如果不真正关注每个人带来的特质及其反应方式，这种平等就难以实现。要知道，要在过程中实现真正平等的发言权实属不易，要让所有人都感到能以充分参与的形式践行这些理想，更是困难重重。各种压迫形式以千百种方式显现。”—— 格蕾丝 9:30

在上述引文中，格蕾丝指出激进社群正在复制更大社会中的权力。尽管激进团体可能试图缓解这些状况，但根深蒂固的倾向难以改变。

女性和有色人种多次表示，她们的发言常被压制、不被重视或遭到忽视。社群内流传的《雷霆集体》刊物《何时该怎么做？3》指出："男性高谈平等的声浪往往淹没了女性的声音。"这种现象导致女性和有色人种的声音无法被听见，尤其当她们表达异议时，更可能感到不适与挫败（Crass）。

一位活动家观察到，在2009年校园占领运动初期，“男性总是不停地站上椅子，发表关于革命的高谈阔论。女性的话语权不断被压

制”（Exposito 2011）。少数小册子合集如《打破枷锁》收录了题为《致运动中其他男性的公开信：闭嘴，或如何在会议中表现更好》的论文，其中列举了若干违反共识的常见行为，包括"将女性发言全部改写，例如'我认为玛丽想表达的是…'" 以及那位"总看不见举手的女性，也从不鼓励沉默者发言"的会议主持人（Spalding 10）。

群体的构成既能决定这些动态关系，也会受其影响。谁加入某个社交圈，取决于现有成员构成、招募方式、社交关系网络及策略。在《她为何对你们的起义不屑一顾》这本小册子中，无政府女权主义作者记录了与一位男性活动家的对话："没错，我们一直在琢磨为何总让女性和有色人种疏远。但我们总在啤酒桌上讨论，这恰恰是问题的根源。问题在于我们从未想到要邀请圈外女性参与政治讨论或其他话题"（《她为何》2009）。

活动人士有时会调整共识流程以确保每个人都有机会被听到。尽管多数团体在会议场合对种族、性别或性取向特权有所认知，但部分团体会明确推行"进一步，退一步"政策，或者更少歧视性的"占据空间，腾出空间" 政策。这些口号旨在鼓励那些通常倾向于保持沉默或者缺乏特权的人"站出来"表达观点。那些观点鲜明或享有特权的人则需"退后一步"，专注于倾听他人。该政策要想见效，发言过多的活动家必须自我反思，承认自身过往行为和特权；而鲜少发言者则需确信自己的声音会被倾听并获得重视。

尽管不常见，但有时组织者会不采用共识决策或绕过该流程。一两个活动家以简化流程、加快进度或保护敏感信息安全为由，为整个团体做决定。这种绕行方式将其他可能持异议的观点排除在讨论之外，可能对女性和有色人种群体产生排斥效应。纽约社区一位活动家就曾遭遇此类情况：她参与联合筹办的"夺回夜晚"游行，次年竟由男性在未经她知情或参与的情况下独立组织。"男性为我们规划路线，未经共识就选定场地、时间和日期 …… 就像亲手烹制的食物被他人嚼碎后喂回自己嘴里"（Exposito 2011）。

分工

激进团体日常运作需要承担诸多职责。活跃成员需维护电子邮件、社交媒体账号和博客，策划筹款活动，制作海报，收集食物，参加会

议，并负责创作、复印、折叠和装订小册子。活动人士常需同时处理多项任务，例如在百乐餐期间丝网印刷T恤，或在团体会议期间折叠小册子。通过共同承担这些任务，参与者得以加深彼此了解，从而建立并巩固社会联系。

当事情通常由成员自行处理时，涉及的劳动量使得平等变得尤为重要。行政事务由核心成员承担，包括查收团体邮件、安排会议时间地点、宣传团体及会议、采购资源以及处理突发问题。虽然这能缓解参与者的流动性，却也阻碍了新成员的持续参与。如果资深活动家不与新成员沟通或没有向其说明具体任务，他们就会缺乏参与能力和意愿。

在许多情况下，开放式团体中核心与外围的形成往往催生出非预期的领导者和非正式的等级结构。活动家们担忧精疲力竭 —— 即因过度投入而导致的倦怠与退缩。然而现实中，大量工作常由少数人承担。为缓解那些不堪重负或考虑离开的成员，必须在现有成员间分配劳动并吸纳新参与者。

许多活动家认为劳动分工中存在性别与性别认同的不平等。尽管刻板印象可能认为女性负责视觉装扮而男性从事"真正"的工作，但在行动主义及其他亚文化领域中，事实恰恰相反。男性在公共空间与公众形象中占据主导地位，例如"占领华尔街"运动的新闻报道（McVeigh 2011）。某些角色与任务能带来更多文化资本，也比其他工作更有趣或更具魅力：集体烹饪与洗碗的区别；为街区派对制作横幅与参加社区委员会会议的区别；在慈善演出摆摊售卖杂志与复印装订两百份杂志的区别。在《转化性正义与/伤害》杂志中，AJ·威瑟斯指出："社区建设的重担主要落在女性和跨性别者肩上。社区组织工作中最重要的部分是建立和维系关系。这种无形且带有性别色彩的劳动在激进组织中被严重贬低"（2014）。

尽管会议机制中已实施应对不平等的策略，但鲜有政策能阻止某些活动人士过度承担任务，或确保公平的分工。唯有在明确以女权主义为宗旨的团体中，我才见到针对此类不平等采取的措施。当成员知晓彼此的个人生活状况时，他们会主动阻止他人承担过多志愿任务而陷入不堪重负的境地。这种做法在《鸟类集体》杂志《你想创建女权主义团体吗》中得到了明确探讨：

> 我们也开始仔细关注谁自愿承担哪些工作，并努力识别和命名那些此前未被重视的劳动任务，例如检查电子邮箱、制定会议议程、主持会议、记录会议纪要，以及主动协助活动筹备的各个环节…… [设立角色] 既能确保成员在集体中承担的责任得到认可，又能避免那些承担超出公平份额工作量的小组成员产生怨气。

部分成员明确表达了对特定类型工作的偏好，或拥有其他成员无法获取的资源，但工作量在成员间得到了公平分配。通过这种方式，当某些成员因个人原因离开时，集体仍能保持高效运作并维持稳定性。

[image]

直接行动

关于直接行动中性别分工的话题，曾在部分黑群运动相关的杂志和访谈中出现。黑群战术主要由无政府主义者采用，参与者身着全黑服装、连帽衫，并遮盖大部分面部。这种装束使行动者难以相互辨识，当然也增加了警方识别个体的难度。

黑群战术同时具有视觉凝聚力。这种美学特征能"向他人表明：只要局势需要，大家已经做好了采取激进行动的准备 …… 因此如果他人希望避免冲突，也能轻易规避"（Graeber，2012）。暴力行为本身虽然没有性别属性，却与阳刚之气高度关联。

这类大规模游行和占领街道的行动催生了"集体幻腾"的瞬间 —— 当人群聚集时，社会力量便迸发出能量与激情，"通过表达这种激情，人们同时强化了它"（Durkheim 218: 1995）。"暴动色情" —— 那些捕捉大规模和/或激烈行动的影像 —— 既唤起"暴动"的反叛感，又暗含兴奋带来的情色意味。观众得以借此间接体验当下的能量与希望。

游行中采取的激进手段和暴力程度会迅速将其基调扭曲为"粗犷而疏离"（Why She 2009）。一位有色人种女性活动家指出，无政府主义者发起的"夺回夜晚"街头占领活动因充斥着粗暴的随意暴力，"更像一场橄榄球赛而非女性主义行动"（Exposito 2011）。这场旨在赋权女性并解决性侵问题的游行由无政府主义女性主导。然而，约30名抗议

者中多数是"身着黑色斗篷和裙装的男性 —— 以此将抗议者女性化"。埃克波西托并非反对暴力，但她指出："把报箱扔到街上确实痛快，没问题。但如果只是一群富有的白人男性这么做，那 ......你们恰恰在重演自己声称要对抗的局面。"同时她更困扰于旁观者更关注无政府主义者的财产损失而非强奸问题。

[image]

性中的性别

性关系

如同其他行动主义群体和社会运动，性关系和/或浪漫关系普遍存在且影响深远（Shepard 2005, Goodwin 1997）。集体沸腾状态、亲密的情欲纽带与性赋权的结合，共同构成了情欲人际关系的理想土壤。正如本·谢泼德在《将欢愉作为社区组织策略》中所指出的，游行活动既是结识魅力人士的场所，也是"寻觅"性伴侣的空间（Shepard 439: 2005）。在激进社群文化中，这种可能性通过连绵不断的深夜活动、音乐演出和舞会得以充分展现。

亚文化中的性规范常被称为"性积极"（sex posi），即性积极态度的缩写，意指性被视为"人类存在中健康且重要的组成部分"（Fuckin’ (A) and Support New York 2012: 4）。对身体、性行为及性取向的自主掌控尤为突出。该亚文化群体推崇追求愉悦的态度与反羞辱话语，但面对"非常规"性行为时，双标问题仍困扰着部分成员。诸如“Not Your Mother’s Meatloaf: A Sex Education Comic Book”等独立刊物，以充满趣味的方式探讨通常被视为不雅的话题，其中包含亲密性体验的故事与插图。性关系与实践已融入社会运动与日常生活之中。

社区内的性取向与实践形式多样。一夫一妻制与非一夫一妻制并存，但规范的模糊性可能导致个体关系中的紧张感。有人讥讽传统关系是主流文化中"性别、婚姻、核心家庭 ... 以及异性恋一夫一妻制"的组成部分（Caytee 21）。因此，参与一夫一妻制关系可能影响个体的文化资本。其他反对理由包括：它在个体间制造隔阂或界限，限制个人性体验，并可能引发对他人控制与占有的念头。与顺性别男性交往的女性或非二元性别者，常发现自身身份被这种关系所定义。某些情况

下，她们仅能通过这种关系获得群体准入资格（Said the Pot, Clementine 2012）。

此外，一夜情、非正式关系、各种形式的多伴侣关系以及BDSM实践也都不罕见。支持者认为，定义关系的能力和灵活性赋予人们以力量。此类关系缺乏先例可循，而《道德荡妇：无限性可能性指南》一书已成为该社群实践准则的非正式权威。这些另类性实践既是对一夫一妻制缺陷的回应，也成为构建社交网络、吸引新成员加入社群的有效途径。

[image]

延伸：The Ethical Slut: A Guide to Infinite Sexual Possibilities
https://ia801900.us.archive.org/13/items/
DossieEastonJanetW.HardyTheEthicalSlutAPracticalGuideToPolyamoryOpe
Dossie%20Easton%20%26%20Janet%20W.%20Hardy%20-%20The
%20Ethical%20Slut%20-%20A%20Practical%20Guide%20to
%20Polyamory%2C%20Open%20Relationships%20%26%20Other
%20Adventures.pd%20%281%29.pdf

物化与“把妹活动家”

女性活动家指出，她们被顺性别男性物化为性对象是反复出现的障碍。正如先前对男性主导亚文化中女性的研究，女性活动家们感到必须向社群证明自己“足够激进”才能获得尊重，同时还要面对被性对象化的压力。团结激励 —— 即其他成员给予的认可与鼓励信号 —— 对持续参与至关重要。

部分女性身份的活动家指出，唯有当她们被"视为性资源"时（**Said the Pot**语），才能获得男性活动家（即实际领导者）的关注。即便展现专业能力，女性在证明自我的过程中仍可能遭遇反弹。知名活动家亚历克斯·雷克曾描述这样一例：她曾帮助一名醉酒男性修理自行车轮胎：

> 我看着他贴好补丁，然后试图三次给轮胎打气都失败了。于是我就主动帮忙。正当我修车时，一群男人开

> 始嘲笑他“居然让女生修车”。他反唇相讥说看女生修车多性感。转眼间他们就围住我，发出哄笑声。而我正帮忙的那个男人假装拿着摄像机，说着要拍女生修车的色情片，还凑近拍摄我用打气筒的镜头。嘲讽的矛头从他身上转移到了我身上，仿佛他的羞耻感被转移给了我”（2007）。

由于一名女性活动家在其他男性面前展现出比男性同事更强的知识和技能，他便贬低她为性对象。她的能力挑战了他的男性气概。对技能和能力的欣赏、认可与赞赏，可能取决于性吸引力或社会资本。

存在一种公认的模式：活动家利用共同的政治立场和亚文化资本来获取性伴侣。这种动态现象普遍到催生了俚语复合词"macktivist"，由动词"mack"（意为进行性暗示）与"activist"（活动家）组合而成。尽管该词在当代口语中可能不再常用，但几乎所有受访者都对其有所认知。此类 "把妹活动家" 通常为顺性别异性恋男性，他们将社会运动作为提升性生活质量的手段。性关系本身并非负面现象，但在"把妹活动家"这里，情欲目标取代了社会运动目标成为首要追求。有受访者特别指出该词暗含"阴暗"意味，暗示其具有故意混淆视听的意图。

"把妹活动家"甚至有时还会自称为“女权主义者”，以此作为获取性伴侣的亚文化资本，伴随着情感操控（吸血鬼）。"有些男人利用反性别歧视言论来勾搭女人"，这引发了疑问：这些男性活动家"在乎的是女人本身还是操女人的机会？"（Tov 2007）。该话题已成为亚文化中漫画和杂志的创作主题。旧金山一位有色人种女性活动家以幽默方式对此作出回应，她列举了"伪女权主义者"的特征清单，旨在帮助女性规避"我们二十出头时约会的所有男性。好吧，还有二十五六岁时约会的那些。好吧，可能还包括快三十岁时约会的那些。但如今我们都懂了"（Kristia 2007）。该清单包括：

「当你们初次在那个时髦叛逆的酒吧俱乐部相遇时，从你们的对话中便不难看出，在此人的嘴里，注入‵社交′、‵约会′和‵组织活动′等等，都统统被归于‵人脉拓展′。″

如果他描述自己的成长经历时总把自己比作世界领袖，那我劝你赶紧撤别犹豫。比如这样：‶你知道吗，就像甘地和胡志明那样，我也是

在大型港口城市长大的。所以对那些城市的多元文化和繁忙节奏，我有相似的体验。”（没错，真的就有个家伙这么跟我说过。）」

"把妹活动家”通常与肤浅的政治斗争“感”有关，即：把特定的文化产物适应性地套用于当下议题的行为，以此作为 文化资本 。

[image]

性关系和/或恋爱关系既能促进合作、成为招募手段和凝聚力的来源，也可能引发群体矛盾、导致疏离感并造成孤立情绪。

人际关系不可避免，它既能强化社会运动的纽带，亦可能削弱这种联系。

知情同意

过去15年间，同意议题在活动家圈子中日益受到关注。性行为规范已从强调"拒绝"转向强调"同意"，同时更着重考量权力差异对决策过程的影响。

各类独立刊物对同意的定义不尽相同，比如：

“同意是指以口头或其他形式给予的许可，允许进行任何可能引发情绪反应的行为，或任何具有‘亲密’性质的个人行为。这涵盖从牵手到性行为之间的一切行为。”（Cheyenne）

“同意意味着所有参与者都愿意并同意在每个环节都保持清醒。在性行为发生前或过程中，你随时可以改变主意。同意意味着所有参与者都明确说'好'！仅凭猜测对方意愿是不够的 —— 这并不安全。”（Generation Five 2006年）

“同意是 …… 在神志清醒（即未处于醉酒或吸毒状态）且充分知晓周围环境的情况下，以口头形式明确表示许可。强迫或胁迫他人发生性

行为，或与处于醉酒、昏迷、神志不清或无法给予同意状态者发生性行为，即构成强奸。"（A D.I.Y. Guide）

"同意远不止于'不就是不'。真正的同意建立在勇于提出关键问题的基础上...以及面对可能被拒绝的勇气。"（Listen 2007: 11）

讨论中的常见主题包括：同意是一个可在互动过程中动态变化的过程，唯有在参与者事先讨论并达成共识时才能通过非语言方式表达，且不可被胁迫。有人质疑口头同意缺乏现实性，但另一些人将其类比于避孕套的争议，例如"这会破坏气氛"（Said the Pot）。激进派同时强调，所有性别的人都可能遭受性侵或强奸，必须给予同意。辛迪·克拉布围绕同意权制定了83个问题清单，该清单被多家杂志转载并收录于她的著作中。

从我整理的小册子样本中可以明显看出，亚文化圈内显然对这个话题有所认知。部分活动家认为相关讨论还不够充分，不过我采访的一位人士表示："关于同意权、强奸、虐待、厌女症、家暴问题行为、权力不平等交换、种族主义、跨性别恐惧症的讨论 ...... 在我参与的社群中，这些话题始终是持续不断的议题...... 我参加的聚会或会议......大概近十年间，几乎每次都会涉及这些议题的某个方面。" (Willow 20:05) 威洛似乎并不认为这种关注度提升是坏事，但她认为亚文化圈里关于"忽视或未充分讨论这些问题"的讨论实属虚伪。

活动人士强调权力动态对同意的影响。正如小册子《并无安全空间：左翼中的父权制》所言："社会整体结构首先决定了我们个人能做出的选择范围"（Cohn and Mitchell 2015: 9）。文化性别动态可能导致女性化社会化个体认为自己不该说"不"，或发现自己无法说"不"。小册子《视而不见 听而不闻 言而不语》的引言写道："我无法总是说'不'，或说'停下，我感到不适'，或说'能慢点吗'，或说'走开'。我的大脑无法完成看似最简单的功能 —— 无法把这些话传达给我的嘴巴。" 对遭受过侵犯的人而言，这种困境尤为复杂。他们"可能陷入僵直或精神恍惚"，"受害者往往难以说出拒绝，因为他们可能觉得拒绝毫无意义"（Cheyenne）。

[image]

返回：

在激进主义文化中，将预示性政治应用于性互动也可能引发问题。性积极文化可能导致行动者感到被迫发生性行为，或将其视为积累社会资本的手段。在某些激进主义文化圈中，人们可能被要求证明自己"足够酷儿"或者"足够多伴侣"（Kirsty, Anna, Hannah and Tasha 2014: 7），如果不积极发生性行为或展现性欲，就可能在社群中感到不受欢迎（Naught: 6）。如今"渴望专一关系已成为禁忌"，人们承受着"迎合多伴侣理想的压力 —— 必须带着伴侣参加舞会派对，还要对伴侣与他人发生关系表现得完全不在意"（Kirsty, Anna, Hannah and Tasha 2014: 30）。普遍认为享受性是优秀女权主义者的特质之一（Traister 2015）。对于参与BDSM的人而言，“同意的界限比其他情境更为严苛。玩伴间所有行为都需事先口头协商，未明确商定的行为即视为越界”（Naught: 17）。

[image]

问题优先级

安全文化

正如上述第三章所述，激进派圈子对保密战术的需求是源于政府间谍在1950至1970年代策划的秘密反情报计划。反情报计划（**COINTELPRO**）通过卧底特工渗透社会运动并实施监控，旨在阻挠行动、诋毁活动人士、制造混乱，全面阻碍社会运动发展。近年案例中，政府雇佣线人或诱使活动人士配合指证他人。

[image]

返回 - 专题栏目：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

外界或许对政府仍在延续 COINTELPRO 计划持怀疑态度，但该计划的威胁性依然存在。国土安全部和国家安全局已承认利用推特、脸书等社交媒体收集反抗团体的情报（Gibbs 2014, Obeidallah 2012）。活动人士采取措施确保信息仅在可信的群体内部流通，避免泄露给政府或其代理机构。行动合法性固然重要，但国安局监控力度的加强与透明度缺失，已使人们对政府潜伏渗透的风险保持高度警觉。

"安全文化"一词指代社区内部对保密性的需求。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

安全文化是激进行动主义文化中所有层面对谨慎性的需求之缩影。它规定了哪些人可以接触敏感信息、哪些人不可接触，以及何时何地可讨论这些信息。行动者将潜在违法或被禁止的战术行动的知情权限制在特定群体内部。对国家通过直接或间接监控实施报复的恐惧，正是这些保密政策背后的驱动力。这类信息可能涉及过去或者未来的事件、行动或人物。

活动家彼此之间不会互相追问私密问题。并且，安全文化默认成员会主动透露希望公开的个人信息。例如，激进社群成员使用化名的情况并不少见，如果向使用醒目化名的人询问真实姓名，或者追问其过往参与过的激进行动/活动，反而会引发怀疑。

关系网络中某些团体及部分环节的非法性质，尤其是激进派社群内的无政府主义派系，都影响着其对新成员的开放程度。出于安全文化考量，活动家的秘密行动本质上具有排他性。

[image]

日常行动在成员间逐步建立起相互信任。

激进活动家对缺乏忠诚纽带或既有社会联系者往往心存戒备。

行动主义所需的情感投入使其易受渗透和操控。

在以破坏性或非法行动为导向的集体中，排他性具有重大影响 —— 对外来者的不信任（尤其是对政府卧底的警惕）可能引发内部猜疑和动荡。

尽管活动家鼓励新人参与，但其目标并非追求大众吸引力。

有时，活动人士甚至会战术性地利用安全文化以忽视其他个人和团体。在内部争执中，女性和有色人种在安全文化的幌子下感到被压制。谁被纳入或排除在外，可能取决于你认识谁 —— 即你的社会资本，以及你是否值得信赖 —— 即你的文化资本。在组织校园占领和学生行动期间，我发现保密性导致多个看似随机的活动家团体各自筹备相同行动，彼此互不知晓。另一群组织纽约市不同校园占领的活动家坦言："没人预见到这种事，因为多数人都没有被邀请。这不是什么新鲜事"（Exposito 2011）。

当女性和有色人种批评组织者未给予他们参与的机会时，那种笼统的"安全文化"回应，往往会质疑反对者对社会正义的承诺及其作为活动家的真实性。批评安全文化可能招致"充当国家代理人煽动内讧冲突"的指控。辩论还可能转向指责弱势群体为“边缘议题”置团体于风险之中。援引政府间谍的"反情报计划"既能诋毁对手，又能维护自身正统性并强行终结争论。

与此同时，正如原论文及后续杂志标题所言，有人指出"[image]为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力 "。在这篇广为流传的文章中，考特尼·德西雷·莫里斯指出："我们必须正视性别暴力、男性特权与线人（及效仿者）破坏激进运动策略之间的关联"（2010）。莫里斯以布兰登·达比为例 —— 这位线人曾伪装成新奥尔良"共同阵地"组织的协调员。尽管其"专横咄咄逼人的组织风格"引发多名女性投诉，却始终未受问责。COINTELPRO另一项与厌女症重叠的策略是迫使活动家采取"更激进直接的行动"（Exposito 2011）。无论他们是否实际担任线人，对社会运动造成的后果如出一辙。

革命之后

部分活动家认为性别议题“次于”更宏大的政治目标。对此的常见论调有二：其一是阶级与政府等更严峻问题解决后再处理"个人问题"；其二是推翻资本主义或政府后性别解放自会实现（Kooky, King 2012, Morris 2010）。在地方层面，围绕这些论点常出现"女权主义分散整体注意力"的说法（Why She 2009）。尽管有时令人遗憾，但性别相

关问题与暴力行为"终究不如那些在社区中延续性别暴力的各族裔男性更重要"（Morris 2010）。正因这些议题动摇运动的团结性，关注者常被视为“破坏者”。正如《近期占领行动》杂志插图幽默地指出的那样，有趣的、促进团结的亚文化实践更有可能被强调。

总体而言，多数独立刊物提出了实现长期社会变革的三种主要途径。

- 其一是：要求行动者将政治理念付诸实践，"开始将自身视为问题所在"（Tov 2007），"在日常生活中支持女性，并向其他男性发声以抵抗性别歧视"（Kooky），"批判性地审视自身的身份认同，同时积极倾听女性与跨性别者的声音"（Ex Masculus 2014: 4），并致力于"无论既定规范或自身幻想如何，都坚持真正的变革与实践"（Men Against 1996: 10）。

- 第二是严肃对待问题并开展预防性工作，例如围绕同意权展开的实践（Mitchell 2016, Rae 2008）。

- 第三是大核心议题在于构建社会运动的包容性 —— 当前现实是"以顺性别男性为主的团体仍将维持其主体性"（Mitchell 2016），"边缘化或多重身份者被迫在入场时割舍部分自我"（King 2012）。

但这些说起来容易做起来难。

[image]

实现这些变革所需的文化转型，需要建立内部批判的框架，使行为得以审视，而不被视为分裂或削弱团结。

社会运动并非独立于其他领域而存在，必然反映出此类不平等现象。

权力等级的复制与部分活动家的边缘化，揭示了追求社会正义的社会运动所具有的复杂性。

[image]

第五章 转化性正义与问责机制

尽管性别歧视及相关虐待与暴力行为时有发生，但社群普遍不愿寻求国家或警方的协助。人们认为政府助长暴力与不公，"系统性地针对并残暴对待有色人种、激进群体、酷儿群体及移民"，因此不可信赖（Erinyen Collective）。监狱的私有化继续边缘化那些已经被边缘化的群体（Davis 2003）。与温和派不同，激进活动家根本不考虑报警选项。解放被视为与废除监狱制度紧密相连，进而要求瓦解整个刑事司法体系。正如《故事讲述与组织项目》访谈在《Miklat Miklat》杂志中所表述的那样："警察就是敌人 ... 在政治层面，你不会求助于压迫者。根本不该这么做。更深层的政治逻辑在于：我们必须找到应对这些问题的办法，而这些办法不应依赖暴力根源本身，对吧？」

即使警方介入，他们也无法识别虐待的多种形式或幸存者的需求。正如运用转化性正义解决儿童虐待问题的组织 Generation Five 所指出的，那些接触刑事司法系统的人"很少对结果感到满意 —— 无论是从幸存者的安全与康复角度，还是从正义感角度而言"，他们既无法免受施虐者或调查程序的二次伤害，"最终得到的只是片面的解决方案，这些方案只会重新掀开创伤，却无法真正转化创伤"（Generation Five 2007: 12）。不仅警方和法院被认为在处理家暴和强奸案件时力不从心，依赖这些机构甚至可能"破坏我们的政治工作"（Mitchell 2016: 21）。

活动家亚文化群体转而 依靠团结和社区力量，要求成员为自身行为负责 。他们认为官僚等级结构无力解决问题，因而追求自主性。为避免政府干预日常生活，活动家们正 创建替代性的社区正义形式，试图建立全体成员相互问责的文化实践 。

对抗性机构必须在亚文化内部需要它们之前就发展起来。对抗性机构的预示政治推动了行动主义文化与生活方式的同构性。活动家们致力于创建反父权制的、反强奸文化的承诺，体现在他们围绕安全、性侵及关系动态建立的反制机构中。某转化性正义团体将其方法称为"通过试错实现革命"（Colman 2009）。由于报警和参与刑事司法系统遭到贬抑，活动家们必须建立替代机制。

替代体系的构建需要大量工作："这不可能凭自发行动实现；它必须源于基于民主、去中心化结构的高度组织化社会"（Beallor 2001）。作为一种DIY实践，大量劳动落在少数个人身上，而他们本身已有其他个人和活动承诺，且成功无保障。

知名杂志《多丽丝》系列作者辛迪·克拉布曾指出：

有时我对替代性机构感到矛盾，因为 …… 它们耗尽了我们所有的时间、精力和金钱，激化最恶劣的权力关系，最终陷入愤怒与绝望，让人不禁质疑其意义何在。但 …… 我认为那些如今被我视为理所当然的真实的替代机构 — 比如强奸危机中心、食品合作社 …… 社区菜园、免费诊所、社区支持农业农场— 足见我们从事这项工作至关重要。必须创造出替代现有生活方式的可行方案”（2011：206）。

辛迪认为，建立成熟的替代性机构——如同前辈们所创建的那样——值得付出努力。当这些对抗性的机构能真正成为警察、法院和监狱体系的替代方案时，其价值尤为凸显。

预防性措施：安全空间

激进主义者的“更安全的空间”

尽管该术语已在主流文化中流行，但在行动主义亚文化中，“安全空间”实践具有特殊的内涵。它常被误解为通过禁止对话来纵容个体；然而在行动主义语境中，讨论的核心在于挑战压迫性结构而非扼杀言论。安全空间是指通过具体策略确保实体空间免受性别歧视、种族主义、恐同及其他意识形态和身体暴力侵害的场所。但安全空间不仅需要消除压迫，更应具备包容性与可及性，就如设置轮椅通道和休息区（Potter 2018）。一旦空间被认定为"安全"，理论上社区所有成员都能在此获得保障。在一份题为“站起来、行动起来”的小册子中，安全空间的宗旨被阐述为三重目标：

> 在个人层面，幸存者免受即时暴力及后续暴力威胁（包括性暴力、经济暴力等）的安全保障至关重要。对社区而言，安全源于培育挑战暴力、支持解放条件的社区规范与实践。最后，在跨社区与集体层面，安全意味着相互问责、挑战群体内部及群体间的权力动态、防范反噬效应，并建立坚实的联盟，使我们能够共同支持与保护彼此，免受国家干预和打压。（Generation Five: 20）

“更安全空间”政策在微观与宏观层面均发挥作用。其被视为一种文化实践，既能应对当务之急，又能推动预示性政治的发展。

更安全空间政策强调相互依靠与构建安全"社群"的重要性。相关信息通过活动宣传渠道传递：包括社交媒体及传单、入口处与空间墙壁及洗手间的海报、活动手册或宣传单上的文字说明，以及活动期间的现场公告。社区成员均被要求参与支持与维护工作，但设有专职协调员负责政策执行，通常通过统一服装或臂章标识，可能驻守信息咨询台。这些政策还便于处理特定个体的请求 —— 无论是处于问责流程中，还是正在规避问责程序。

如果“更安全的空间”政策受到违反，个人和社区都被视为受损。针对空间政策违规行为的处理规范已逐步形成：相关人员首先倾听受害者的陈述，并立即确保其安全，有时会要求违规者离开该空间。随后询问受害者期望采取的行动方案，并评估社区整体安全状况。受害者可选择三种应对方式：要求"对该人员进行监护"、与当事人沟通行为问题，或要求其当晚离开活动场所（Potter 2018: 15）。如需采取行动，将由双方指定联络人进行简短调解。由于参与者均知晓该政策且基于社区共识，驱逐安全空间违规者时极少需要使用强制手段。

在活动人士频繁活动的多数场所，均可建立安全空间机制，仅有少数例外情况。此类机制是预防伤害或及时应对伤害的核心手段。部分组织者创建了 NYCsaferspaces.com 网站，为其他试图制定自身政策的活动人士提供参考资源。诸如纽约无政府主义书展等年度社区活动已确立相关政策，在活动手册中附有书面条款，并与安全空间团体协作执行。

以下是我作为"支持纽约"成员协助制定的第五届纽约无政府主义书展

安全空间政策：

如果您在活动期间遭遇骚扰、虐待、侵犯或其他任何形式的侵害，或有人实施此类行为影响到您的参与体验，或因任何其他原因需要支持，请立即联系志愿者。现场配备受过专业培训且经验丰富的倡导者和支持人员，可协助处理此类问题。

本政策旨在认清并抵制强奸文化作为社会常态的现状。所谓强奸文化，即纵容、开脱甚至鼓吹性侵犯及其他性暴力行为的文化环境。强奸文化植根于更广泛的暴力文化体系，该体系通过社会化过程使人们在等级关系中占据不同位置，将他人商品化，并以暴力胁迫维系人际关系。强奸文化的延续、体验与应对方式，与其根植的父权制、白人至上主义、资本主义、恐同症及殖民主义等压迫体系密不可分。

我们致力于以幸存者为中心，以幸存者为导向。当需要在给予实施虐待行为者"无罪推定"与支持幸存者之间作出抉择时，我们将优先支持幸存者。

如果根据本政策要求您离开书展，请立即离场。如需讨论该决定的原因，可预约活动结束后进行沟通。

该政策虽针对具体活动制定，但植根于强奸文化与"压迫体系"的意识形态和政治语境。它预见了潜在冲突，并明确无误地站在幸存者及受害者立场予以支持。其他形式的框架曾在集会和群众行动中应用。例如，我采访的一位参与者曾协助将安全空间响应机制适应抗议场景。为筹备集会，他们组建了性侵应对小组，并设立专属热线和维基页面，以即时有效处理性侵案件。此外还设立了指定的“更安全空间”，供活动人士寻求援助。

[image]

复杂性与局限性

“更安全空间”最大的问题之一就体现在其名称上。最初这些空间被称为"安全空间"。然而活动家们不得不承认，“安全”无法得到绝对的保障。主流文化中的不平等现象必然存在，尽管活动家们在竭力消除，

却无法根除。活动家们开始将这类空间称为"更安全"的空间，以承认社交互动和激进行动中固有的持续风险。术语的转变也为进一步的批判、讨论、承认缺陷和调整留下了空间。

大型团体往往难以达成政策共识。以"占领华尔街"运动为例，其“更安全空间”政策制定过程就充满波折。该运动汇聚了经验丰富的活动家和大量初涉者，政治理念横跨个人主义自由主义到集体主义社会主义。受访活动家伊娃曾参与制定占领运动政策：

制定安全空间政策耗时五个月 …… 但我们确实召开了全体大会，让每个人写下了他们期望的政策框架，与各方深入探讨了大家的顾虑，随后又与发言人委员会反复研讨 …… 结果最后却遭遇意外 — 听障者组织团体告知我们该政策过于复杂，难以翻译成手语 …… 整个过程堪称一场漫长征程。但我们确实通过了这项政策，所有人都感到无比振奋 …… 我们当时说：‘不，各位，这只是开始。接下来还有更多工作要做。’可惜我们没能推进后续，因为占领运动逐渐失去地域集中性，组织模式发生变化，我们也精疲力竭了。不过我们确实通过了政策，这算是个开端。”— Eva 31:15

伊娃加入占领运动时已具备推行“更安全空间”政策的经验。但由于占领运动规模庞大，政策协商过程尤为艰难，历经工作坊、培训、各类小组会议、政策调整及磋商环节。

这些政策还需清晰传达并切实执行。当新成员不了解既有动态、人际关系及个人行为模式时，往往会引发冲突。典型案例是某争议性男性活动家主导的小组，曾否决一场女性主义与有色人种主题的杂志活动。该小组展位人员均为初涉此领域的女性，而活动组织者来自朋克及有色人种运动圈层，对自由主义者和自行车团体了解有限。双方均不知该团体由一名白人顺性别男性领导 —— 此人曾被指控施暴、逃避责任并报警针对有色人种。该男性当日未出席，我们多以为他已退出团体。但事实并非如此，主办团体发表邀请声明后，引发所有相关团体通过邮件及网站展开交锋。

虽然多种空间类型都能变得"更安全"，但学术机构存在独特的复杂性和局限性。校园内时常发生活动家集会和抗议活动，即便参与者未必

全是学生。由于学校空间部分由国家资助，且嵌入更庞大的官僚体系、政府机构和资本主义权力结构之中，其制度权威便由这些结构所界定。踏入校园时，保安人员、监控摄像头、签到制度和身份证件便向我们昭示了这一点。当出现人身安全威胁时，多数学校的应对指南要求立即联系安保和警方。校园中还普遍缺乏组织性支持。这项工作需要有奉献精神的人士在学术社群中持续巡查，宣传并执行“更安全空间”政策。

[image]

延伸：https://iyouport.substack.com/p/c3b?utm_source=publication-search

延伸：https://iyouport.substack.com/p/2025-a7f

延伸：https://iyouport.substack.com/p/1012025

批评

许多受访者认为政策在执行时过于简单化。仅靠张贴"禁止性别歧视"或"禁止种族歧视"的标语，无法解决深层的复杂问题。一位受访者将这些政策比作公共泳池的规则：

"我觉得这种说法有点太简单化了，比如—— ‵不要性别歧视′——毕竟我们身处根深蒂固的性别歧视文化中；或者说‵不要种族歧视′——毕竟这个国家建立在奴隶制基础上。要解开这些纠葛实在太难了，尤其当你面对的不过是泳池里那种‵禁止嬉闹′‵禁止跳水′的告示牌时。” 38:15 Mary

对这类空间的批评常指出其流于形式 —— 鲜有活动家会将自身行为视为性别歧视、种族主义或恐同行为，即便他人可能如此认定。关于“更安全空间”政策过度简化的争议还包括：此类政策可能导致"诸多本应解决的动态关系"再度重现，而非实现"建立促进建设性对话框

架"的根本目标（Rachel 2016）。政策基于禁令的本质意味着问题与危险并未被解决，只是从这个空间转移到另一个空间。

另一些人对“更安全空间”政策持悲观态度，因为这些政策仅作用于个体层面，处理个人互动问题。发表于数种杂志的《安全是种幻觉》一文指出，安全"无法在社区层面被调解或盖章认可"，而是取决于个体及其互动情境（Celeste 2014）。在访谈中，玛丽后来向我讲述了她最糟糕的安全空间政策经历：她和其他组织者不得不耗费大量时间处理两名活动家的沟通事宜：

有人来找我们说，名单上的某个艺术家是性侵犯者…… 这件事让我们吸取了教训，我们试图了解完整情况并询问当事人，结果简直像噩梦一样。

最终我们直接告知双方都不要来，因为我们不想……不想惹上麻烦，当时局势实在太过动荡，对任何一方都不会有好结果…… 虽

然这也不是最佳解决方案，但当时我们实在别无选择……这大概是我执行安全空间政策最糟糕的经历……毕竟你不能置身事外，不能说"这不关我事，你们俩的纠纷自己解决"。虽然我对当时的做法感到不安，但更无法忍受邮件链中四处飞溅的指责，以及他们之间的纷争消耗了大量会议时间—这完全适得其反……我只是觉得人们太容易陷入两三个人之间琐碎的纠葛，却忽视更深层的影响。

当你只是反复贴创可贴敷衍了事时，伤口只会不断涌现。” 玛丽书 40:13

玛丽的经历并非个例。如果流程没有明确建立，便缺乏沟通链条，处理此类问题时难免令人沮丧且徒劳无功。当活动人士深陷激烈争论的细节时，虐待和袭击事件便可能被简化为"闹剧"。

[image]

问责制

转变性性正义之前

在转变性正义模式实施之前，社区正义意味着活动家造成伤害后会被驱逐出社区。活动家往往流动性强，当被要求离开时，他们可以简单地迁往另一座城市，融入新的社区。"如果给所有犯错者都买张去内布拉斯加的单程车票，这个圈子很快就会变得非常小。而奥马哈的居民恐怕不会觉得有趣"（《关于社区的思考》2008:3）。这种驱逐方式将施害者"妖魔化"，反而可能使其在新环境延续不当行为（Erinyen Collective）。

另一种选择是忽视或否认这种行为。有时结果是幸存者选择离开；“根本无从谈起，没有空间去处理这些‘私人问题’，所以我们只能离开”（Colman 2009）。另一种选择是女性通过小册子记录亲身经历。"如果遭遇性侵，你只需写本小册子，详细揭露施暴者的卑劣行径，呼吁众人与之断绝往来并将其驱逐出社群。通常每个城镇都至少会有一两个人认真对待此事……"（《思考过程》）。其中最具影响力的当属2003年由两位女性创作的题为《宝贝，我是个大男子主义无政府主义者》的小册子，针对波士顿某位具体活动人士的行为展开批判。该册子收录了当事人之间的电子邮件及网络对话记录。当受害者希望继续参与活动却认为自身遭遇未被重视时，部分幸存者开始对性侵行为进行反击。在《多丽丝》第21期中，辛迪·克拉布谈及1990年代初期的女性团体：

女孩们重新定义了强奸，突然间所有经历都变得重要起来。发生在我身上的所有糟心事都变得重要了，她们让这些经历变得真实。

继兄的手算数，那个曾逼我给他口交的唱片店老板算数，保罗在我母亲厨房从背后侵犯我也算数，那个男友每次威胁"不从就找别人"时我被迫与他发生关系也算数。街头那些猥亵言语，所谓的‘不经意’的揩油 …… 报应时刻到了。你能想象这句话蕴含的力量吗？”（Crabb 2018）

这些攻击发生在"暴动女孩"音乐兴起和新一波女性主义赋权浪潮期间。总体而言，这种应对方式并非所有受害者都能获得，且执行不

一，未能在激进主义/无政府主义亚文化中引发重大变革。进入21世纪初，以《多丽丝》系列和《支持》为代表的反侵犯杂志，推动了围绕同意权与虐待行为的更广泛文化变革（Accounting for Ourselves 2013）。

修复性与转化性正义

在转化性正义兴起之前，修复性正义曾是社区正义项目的核心。修复性正义着重修复关系而非惩罚行为。"修复性正义是涵盖各类项目的统称，旨在让受害者、侵犯者及社区成员共同应对侵犯行为造成的伤害。其内涵既包含核心价值观（如赋权、疗愈与开放），也涵盖实践方式（如面对面交流、开放对话、参与式介入等）」（Woolford and Ratner 2010: 6）。

该理念着重关注幸存者的需求；"修复性正义程序的目标更倾向于使所有相关人员能在同一社区中安全、尊重地共存，最重要的是让受害者得以疗愈创伤，在感受到支持、尊重与安全的社区环境中，以自己期望的方式继续生活"（“Restorative Justice…”: 13）。

修复性司法基于某些原住民社区的现行实践；然而这些实践并未被普遍采用，相关讨论往往抹去了内部的文化差异（Withers 2014）。纪录片《空洞之水》讲述加拿大奥吉布瓦原住民社区应对儿童性侵的历程，常被从业者推荐。近年来，传统保守的社会机构（如公立学校）开始采用该术语，且"常将其置于辅助体系中 —— 在更广泛的刑事司法体系内维持特定功能"（Woolford and Ratner 2010: 6）。

转化性正义作为一种社区正义方法，与修复性正义极为相似。但在保持以幸存者为中心关注的同时，它更强调施害者个人转变以及导致虐待行为的更广泛的社会不公问题的解决。转化性正义还"承认一个人既可能是受害者，也可能是施害者"（Femme Left）。实践中，修复性正义与转化性正义差异不大，但"修复"虐待关系与"转化"虐待关系的表述差异，呼应了旨在对抗社会压迫的行动主义预示性政治实践。

致力于解决儿童性侵影响的组织"第五代"将转化性正义的目标列为：

- 幸存者的安全、疗愈和能动性
- 施害者的问责和行为思想转变
- 社区行动、疗愈和问责
- 转化/变革使暴力永久化的社会条件 —— 压迫和剥削、统治和国家暴力的系统（Generation Five 2007）

在实践中，转化性正义常以问责程序的形式呈现。问责程序具有灵活的运作模式，可由受害者、社会运动团体、社区或施害者主动发起。对个人而言，其目标在于让施害者为自身行为承担责任，使其承认并接受责任，并承诺未来改变行为。作为社区程序，参与者包括伴侣、朋友及同为活动人士的伙伴。转化性正义组织如第五代（Generation Five）、激进女性主义组织INCITE!及反强奸反虐待社区联盟（CARA）等，早期制定的指南对激进主义亚文化中的转化性正义实践产生了深远影响。

作为行动主义中的问责机制

转化性正义模式正被用于处理已发生的伤害。在亚文化圈中，施害者的转变通常被称为"处理自己的问题"或"解决自己的问题"。这些过程几乎完全围绕性侵犯、亲密关系中的肢体暴力及情感虐待展开。其他形式的伤害可能通过集体干预等方式进行处理，例如针对酒精和药物滥用的干预模式。但活动家们仅在涉及浪漫关系或性创伤时才会被要求"承担责任"。

所有个体都可能相互伤害，施虐者亦可获得救赎。"他们相信互助解决问题，承认人人都会犯错，且都可能犯下重大过失 —— 尤其是在这个他们称之为文明的病态和扭曲的环境中长大的人。要真正改变现状，唯一途径就是互相指出问题，然后学会下次做得更好"（Erinyen Collective）。激进左翼社会运动的预示性政治要求社群携手互助，扶持那些"渴望支持且有意改变自我和处境的人"（《社群思考》2008）。

在激进左翼活动家亚文化中，最具直接影响力的组织之一是"费城挺身而出/费城愤怒者"。这些团体源于2004年一场朋克音乐节上多起强奸案引发的讨论。"费城愤怒者"（PP）是致力于幸存者支持的女性团体。"费城挺身而出"（PSU）则包含男性成员，并在成立首年经历了重大转折 —— 一名创始成员因性侵指控遭到公开谴责。约30名活动家参加的会议上，几乎所有人都在为被控者辩护。结果下一次的会议仅有两人出席。由此，这个"曾经由异性恋和隐秘同性恋男性组成的庞大团体 ... 蜕变成为由公开酷儿和性别非二元成员组成的紧密团体。该组织首次实现了去白人化"（Kelly 2012: 46）。

PSU与PP的职能逐渐分化，最终形成PSU"处理施暴者"、PP关照幸存者的分工（Kelly 2012: 47）。PP于2008年解散，PSU则在2012年停止活动。正因PSU和PP早期发行的刊物与指南，我采访的几乎所有受访者都将该组织视为早期启蒙力量。

大约同一时期，"支持纽约"（SNY）组织从纽约市的朋克/无政府主义亚文化中应运而生。该集体成立的宗旨是"支持性暴力幸存者，教育自己与他人认识性暴力及亲密伴侣暴力的危害，探索在不诉诸警察和监狱体系的前提下如何应对——这些体系只会加剧压迫与虐待"（Support New York）。该组织早期同时处理幸存者与施暴者（集体采用的术语）相关事务，并开展干预流程。随着经验积累，SNY逐步建立流程框架、明确流程中各方的职责，并开发出配套课程体系。该组织于2016年初停止主动开展干预流程，并于2018年将课程体系发布至网络平台。

[image]

三大组成部分

A 幸存者

尽管存在多种形式的性别歧视、种族歧视及其他不平等现象，问责制却几乎完全围绕性侵或亲密关系暴力展开。在我进行的访谈、阅读及个人经历中，仅听说过一起以种族问题为起点的问责程序。截至2018年9月，该程序仍处于筹备阶段。该亚文化群体涵盖多元性别认同，普遍反对性别本质主义，因此承认"任何人都可能跨越性别界限实施侵

害与虐待"，尽管男性认同者可能更不愿承认虐待行为（《为自己负责》2013:5）。但同时必须承认，主流模式仍是顺性别男性对女性、非二元性别者或跨性别者的伤害（Accounting for Ourselves 2013, Betrayal 2012, Withers 2014）。跨性别活动家A.J.威瑟斯在其记录性侵经历的杂志中，阐述了性别认同的复杂性与幸存者身份的矛盾：

我在多伦多的激进主义圈子里遭遇过几次性侵犯，无论我当时如何自我认同，每次事件都带有强烈的性别色彩。
无论是否与我的跨性别身份相关，我深知施暴者将我全部或部分视为女性的事实同样构成侵害根源。

但我的遭遇 —— 当男性气质被抹杀或贬低时遭受侵犯 —— 并不代表所有跨性别男性/性别酷儿群体都面临相同处境。部分跨性别者遭受性侵纯粹因其跨性别身份。

此外，我提及自身遭遇部分源于被强加的"女性特质"，并不意味着在讨论性暴力时可随意将我归入"女性"范畴。我并非女性，将我归入该类别即属跨性别恐惧症。"（威瑟斯 2014: 14）

将"幸存者"一词用于指称受伤害者也存在一定争议。相较于"受害者"，"幸存者"是1980年代女性主义运动中兴起的重塑叙事的一部分（Sehgal 2016）。选择"幸存者"身份，意味着强调经历侵害后展现的坚韧而非受害者的脆弱。"幸存者"一词"指代应对创伤并继续前行的能力；将创伤事件融入生活语境并予以接纳，而非回避或'掩埋'事件"（Cheyenne 5）。然而核心术语的转变可能迫使受侵害者感到：他们“不能”展现脆弱，“不能”按自身节奏疗愈，必须强装坚韧。在亚文化圈内，我还没有发现任何替代性表述。尽管有时带有批判意味，但所有受访者在自我认同时都使用了"幸存者"一词，即便他们本人拒绝接受这个标签。

在进入疗愈过程之前，幸存者需识别或"揭露"虐待行为。该亚文化群体将虐待的定义扩展为"造成伤害的行为"（Wrekk 2007），或"侵犯个人边界的情形"（Crabb 2009）。除身体虐待外，此范畴还涵盖性虐待形式或"将性行为作为武器"的行径，包括"侵犯'性器官'……强迫参与或观看色情内容、无视安全词"（Unowho）。亚文化群体中普遍承认，界定强奸行为"困难重重"（The Down There Health Collective:

11），或"因经历本身混乱而难以厘清"（Cohn and Mitchell 2015）。

通常而言，强奸被定义为"任何形式的非自愿性接触，其界定标准由幸存者本人决定"（Dealing with Our Shit Collective: 5），尽管这涵盖了"无数种情境"，包括围绕非单一伴侣关系、多伴侣关系及性积极态度的文化压力（Soph：5）。众多活动家已呼吁为这些情境创造新的/更丰富的表述方式：

> 或许我们需要一百个新词来描述当朋友、熟人或伴侣侵犯或强奸我们时的情形。一个词形容"我放任你，因为当时半睡半醒，累得无力反抗"；一个词表达"我厌倦了为此争执"；蚝油一个词指代"你对我说话的方式既扭曲又可怕"。一个形容'我明明说过不想那样'。另一个形容'你为何没察觉我早已不在状态'。再一个形容'我们约定过要采取保护措施'。还有一个形容'你说过如果我不从就会离开我。我还有什么选择？”或许我们需要创造上百个新词来谈论强奸、性侵犯和性操控 —— 这些词语必须清晰揭示施暴者对我们身体所作所为的严重性。又或许我们的朋友、熟人和伴侣需要鼓起勇气去听见‟你强奸了我”或‟那是性侵犯”这样的控诉。（Crabb 2016: 49）

由于激进主义者通常采取另类的性实践，围绕“知情同意”就产生了独特的问题。当BDSM关系中支配方没有遵守安全词、忽视其他身体信号、没有提供充分事后关怀，或当多伴侣关系中违反安全性行为协议时，便可能构成虐待。

与刑事司法体系不同，转化性正义亦承认情感虐待的存在。情感虐待被定义为"通过贬低或伤害他人而施加权力"（**Unowho**）的行为模式，或通过胁迫"迫使他人违背意愿或理性判断行事"（Wrekk 2007）。情感虐待虽在活动家亚文化圈外获得认可，却未被刑事司法体系视为严重或可追责的行为。

在激进派圈子领域，识别虐待行为尤为困难 —— 既因其在运动语境中呈现出特殊形态，也因这意味着必须承认被视为“政治道德典范者”实施的虐待。其中一个典型模式是：受虐幸存者被利用来推进施

虐者的政治事业，将"自身的一部分 ... 奉献给他人的事业"（Wrekk 2007）。在某知名案例中，一位幸存者描述其前夫"利用 [她] 自己的政治立场来对付 [她] "，操纵她改变性行为和消费习惯以迎合他的政治主张。她被灌输"不够激进"的自我怀疑。

情感虐待的其他形式包括言语攻击、精神操控、情感隔离、施压参与高风险行动、自残威胁及破坏财物（Cohn and Mitchell 2015, Regarding ********, Thoughts on Possible 2013）。

在 [image]为什么说厌女者最容易成为出色的警察线人？—— 性别暴力如何助长激进运动中的国家暴力 一文中，作者讲述了她们与施虐男性的经历：

> 在我们主办的夏季聚会上，有人当着一群有色人种青年的面骂他的女朋友是婊子。那个在墨西哥旅行期间性骚扰一对墨西哥裔同性恋情侣、还试图迫使他们玩3P的人。那些说要完成任务却不去做的人，对同伴的问责要求不屑一顾，让其他女队友接手任务，而任务完成后却把别人的辛勤劳动全部归功于自己。那个打了自己伴侣的研究生 —— 大家都知道是他干的，但每当有人问起，大家都会一脸羞愧和尴尬，喃喃自语："这很复杂”。

[image]

辱骂、性胁迫、打嘴炮摘桃子窃取他人成果、甚至肢体暴力 —— 这些都是激进主义社群中真实存在的虐待形式。情感虐待被公认为该亚文化圈中的重大问题，"值得获得远超当前关注度的重视"（Cohn and Mitchell 2015: 12）。

有人认为情感虐待在关系中具有内在的相互性。通过使用相同的术语和流程，各类虐待行为被等同混淆。受访者威洛对此提出批评："人们总觉得需要证明自己受了多大伤害，但我认为更合理的做法是关注不健康的权力交换，帮助朋友理清问题，而非使用如此夸张的生存叙事话术"（10:40）。威洛还担心，在这种亚文化中充斥着年轻化和派对氛围的环境里，很少有人能经得起行为的严格审视。

另一些人则认为质疑情感虐待的有效性，是另一种形式的“受害者指责”，会淡化幸存者的经历（“Safety is an…”）。部分活动家质疑将创伤分等级的做法 —— 这种做法将某些形式的创伤量化为比其他形式更严重，而另一些人则批评将各种虐待形式等同对待的做法（Bayer 6）。围绕情感虐待的相对重要性存在一系列的分歧。有人认为社群必须承认情感虐待是合法创伤，也有人认为活动家需要以不同方式应对不同形式的虐待（Cohn and Mitchell 2015）。

与国家司法不同，激进派社群的问责程序以幸存者的需求为核心。组织者认为幸存者"应当决定问责程序的形式与运作方式，以避免二次伤害并恢复幸存者的自主权与自主性"（Brown 2013）。通常情况下，幸存者参与的动机是阻止施害者继续实施侵害行为并伤害他人。尽管幸存者并非总是参与程序的一方，也并非总是发起程序请求的主体。虽然较为罕见，但偶尔也会由社会运动团体或者施害者本人提出程序请求。

采用转化性正义模式时，识别虐待不需要举证责任。受害者与施暴者的二元对立被打破，正如某本杂志部分标题所言："我们都是幸存者，我们都是施暴者。" 单一真相受到质疑，取而代之的是对相关者经历的认可。"任何人都不应被迫为自身感受辩护，尤其不该要求那些经历过边界侵犯的幸存者如此。无论'真实发生什么'，个体的经历都属于他/她自己"（“We are all…” 2005: 39 ）。

在深受国家文化影响的社会环境中，这种观念转变颇具挑战。但部分活动家将其与传统阶级不平等议题相类比："当听到工人罢工时，你不会要求证明老板的过错 —— 而是思考如何最好地支持工人"（And What about Tomorrow? 2009）。

但部分受访者在应幸存者要求执行干预程序时遭遇了困难。李在推进干预过程中发现，虐待行为/事件已被融入这对伴侣的常规性行为模式。最初描述的情节相当骇人：幸存者入睡时告知伴侣不确定是否愿意发生关系，醒来时却发现对方正在"强行侵犯"。" 直到两三个月后才发现，这其实是他们关系中某种'默认同意'的模式 ... '睡醒就做'并非不可触碰的禁区，恍然间意识到'噢等下，这完全是另一种语境'"（13:30）。此案例中幸存者并未说谎，但是非对错的界限却在灰色地带被重新划定。

阿斯敏也有类似经历，她觉得自己参与的问责小组 “在正确评估事件真相方面不够审慎……好吧，你们相信幸存者 …… 把他们的陈述放在首位，这没错，但这反而导致了一些臆断。因此我们根本不该追问施害者对此事的感受，因为这会为误解或诋毁留下空间 …… 我们俨然成了国家机器，成了警察……这绝非否认实际伤害的存在及应承担的责任"（16:25）。只考虑一方观点而质疑另一方是教条主义。由于过程缺乏细腻度，幸存者/施害者的二元划分本身就容易限制转变的可能性。

[image]

施害者

造成伤害的人通常被称为“施害者”，尽管这个术语存在争议。

“费城挺身而出”组织指出，他们“最终采用‘施害者’一词来普遍指代性侵事件中与幸存者对立的人。我们采用此术语，是因为它体现了对行为主体的认知 —— 强调其实施了特定行为，而非本质属性。这种表述既承认其行为造成伤害，也为改变提供了可能”（费城挺身而出组织）。

由于该组织是推动此类实践最具影响力的团体之一，其他倡导变革正义的活动团体纷纷效仿。诸如"施虐者"等术语则暗示当事人本身具有恶性本质，因而无法改变。同样地，"袭击者/施暴者"暗示施暴者体能更强且性侵行为系预谋。该词还暗示存在暴力行为——尽管并非所有案例都涉及暴力，但确实可能存在。因此我选择使用"施害者"一词——无论有意无意，其行为都给他人造成了创伤（Cheyenne 5）。

尽管多数团体使用该术语，但它备受批评。具体而言，人们认为它具有"法律色彩，并可能 …… 重构某种司法体系"（The A Team 2014）。尤其当缩写为"perp"时，该词更复刻了监禁系统的术语体系。反对该标签的活动家们指出，尽管并非本意，它仍会给当事人贴上标签，并在活动家亚文化中形成一种主导身份。尽管不如"强奸犯"这类污名化标签尖锐，"施害者"对处于转变过程中的个体而言仍是难以接受的身份标签。受访者詹姆斯曾参与一个转化性集体组织，该组织采用替代性表述取代"施害者"：

我们不愿使用“施害者”这个词，因为我们工作的本质在于……与施害者建立信任，而称呼他们为“施害者”无助于此。同时这也关乎破除对施害者身份的神秘化认知——他们并非你脑海中刻板印象中的施害者原型……也不是潜伏在暗处的陌生人。所谓的施害者往往是日常生活中相当友善的人……采用不做人格定性的表述更容易沟通。他们确实实施了虐待行为，但未必就是'施害者'——这种语义上的微妙处理实则是信任的工程，旨在呵护我们希望帮助的对象，因为最终目标是让他们不再伤害他人。'施害者'这个词听起来像警察用的……集体里有些人开会时仍会用'perp'这个缩写，因为我们都偷偷看过《法律与秩序：特殊受害者》，这成了集体成员的集体羞耻宣泄—— 每周看着Ice-T痛殴强奸犯，以及 ……幻想警察系统真的关心幸存者，这种怪异的情结莫名吸引着我们所有人……"

亚文化圈中的其他成员则认为，对该词的敏感性属于"旨在迎合施害者辩护策略的问责机制"（Betrayal 2012: 11）。尽管我个人认同针对"施害者"一词的大部分批判，但本研究仍采用该术语，因其在亚文化圈中最为普遍。

团体及独立刊物中使用的替代表述包括"施虐者"（INCITE! 2005）、"施暴者"（Withers 2014）、"侵略者"（CARA）、"造成伤害者"（Creative Interventions）以及暴力"实施者"（Support New York）。施虐者、袭击者和造成伤害者等术语较为直白，此前常与施暴者并用。持续施暴者一词由纽约支持组织倡导，旨在表明暴力与父权制的延续性，并围绕打破这些循环及"更大的压迫体系"的延续建立问责机制（纽约支持组织）。小册子《亲密暴力社区应对方案探析（修订版）》则完全摒弃语言表述，采用三角符号代表"幸存者/指控者/受害者"，四角星符号代表"施暴者/被指控者/最明显的问题根源"（第7页）。

当面指出某人行为不当是非常复杂的。在亚文化圈内，围绕"公开谴责"与"私下劝诫"两种文化理念存在诸多争论。"公开指责文化"被定义为"一种充满毒性对抗的文化，通过羞辱他人来应对压迫性行为，其本质更像是正义的表演而非真正追求公正"（Cheng Thom 2016）。但即使批评者也承认："有时公开点名是应对有害行为的唯一途径，尤其当当事人之间存在权力失衡时，私下沟通无法解决问题" （Ahmad 2017）。而"私下劝诫"则意味着"召集犯错并造成伤害者…与我们共同

探讨其过失，协作制定避免重蹈覆辙的策略"（Rachel 2016: 3）。无论哪种方式，初期反应往往充满波动。

在接受《变革正义》欧盟版采访时，安娜·沃谈及其中的困境：

这就是最初的挑战，我至今仍在寻找委婉表达"对方认为你是施害者"这句话的方式。无论如何传达，通常都会引发相当激烈的反应。因此当这种情况发生时，我会尝试用他们能理解的类比来解释。如果了解对方的生活背景，我会将其类比为令其产生受害感的场景—比如骑自行车时被汽车司机突然横插。我知道这听起来很肤浅简单，但有时必须用不具威胁性的外部例子来阐释。"（Vo 2011）

幸存者或组织可以公开谴责施害者。在我们的访谈中，长期参与问责小组的詹姆斯发现，早期讨论多围绕"亲密关系中的性虐待和情感虐待"。但到了中期和后期，人们开始被伴侣公开谴责，同时也会遭到所属集体的集体谴责（15:25）。

最初反应往往包含否认和辩解。我采访的目击者描述被点名者"惊慌失措"、"震惊不已"，使用"否认和说辞"，并称幸存者"疯了"。在《我想变得更好》一文中，一位被点名者坦言："当时我没意识到严重性。他们错了！是他们的错！如果他们言行稍有不同，此事绝不会发生！这套行为模式我从未察觉。我从不那样行事，我是女权主义者。是盟友。是无政府主义者」（Rose 2015: 15）。一位在担任初始联络人方面经验丰富的受访者表示：

"这个过程需要很小心翼翼地试探，努力不要惊扰到对方，因为他们就像受惊的马匹般敏感……同时还要跳一段微妙的性别之舞 — 既渴望被认真对待（这意味着要展现男性气质），又希望这种表现方式既不违背自我认知，也不强化父权体系。这其实是场极其艰难的舞蹈……” 42:30

转化性正义的目标之一是让受害者与施害者共同留在社区中。所有相关人员都必须相信施害者具备自我反思的能力，能够在未来改变行为。既要充分认识行为模式，又要对未来改变抱有希望，这种能力往往相当复杂。

在前述《我想变得更好》一文中，施害者谈到了自身转变的需求：

"我与调解员存在分歧的一点是……当他针对我的行为说'这已构成你的一部分'时。不，并非如此。虽然我理解他想表达的——我不应逃避过往，自我完善与责任承担是持续的过程 —— 但为何这些身份标签必须成为我的本质？为何不能成为过去的一部分？如果缺乏责任承担过程及整个社群赋予的重塑身份的机会，人们便缺乏践行责任的动力。如果我们给每个人贴上无法康复或修复的标签，便彻底丧失了实现真正正义的希望，反而会重构我们试图瓦解的旧体系。"（Rose 2014: 14）

被指责者必须相信自己能够转变。否则，施害者参与这个过程的唯一动机就仅剩下维持TA自己在群体中的地位了。

转变过程的根基在于这样的理念：每个人都有可能成为施害者，因为"即便是最优秀的人也可能犯错"（Naught and Rachel: 22）。如《当你被指责时该怎么做：简明指南》、《迈出第一步：给因虐待行为被公开指责的人的建议》、《当有人告知你侵犯其边界、令其不适或实施侵害时的应对指南》、《我们皆是幸存者，我们皆是施害者》等等指南，既阐明任何人都有可能实施虐待行为，也强调了处理此类行为的重要性。这些指南通常包含"为自身行为负责"和"寻求帮助"等核心建议（“We are all…” 2005）。

其中最广为人知的《迈出第一步》被诸多其他杂志转载，为被指责者列出十条建议：

1. 保持诚实，坚持诚实，学会诚实

1. 尊重幸存者的自主权

1. 学会倾听

1. 保持耐心

1. 永远、永远不要责怪受害者

1. 为自己发声

1. 不要保持沉默

1. 不要躲在朋友背后

1. 响应幸存者的意愿和社区的意愿

1. 勇于担当。在暴力与侵犯发生前阻止它们。

最常用的说法是施暴者需要"处理自己的问题"或"解决自己的问题"。这通常意味着他们需要改变行为，但具体含义却模糊不清。要实现真正的转变，施害者必须"同时满足两个条件：**a)** 真正渴望获得支持，**b)** 有意愿改变自身及/或所处环境"（Thoughts on Possible 2013: 6）。

对部分有实践经验的活动家而言，唯有施害者真心求变才值得投入精力："初入此领域时，我曾耗费数小时跟一个人单独会谈，等待其产生共鸣。如今我逐渐掌握了放任顽固者的技巧，转而投身更易促成改变的领域"（Vo 2014: 55）。部分批评者认为，要求施害者"'处理'其男性身份、重塑阳刚气质表现……调整男性角色定位"的做法，实则强化了父权文化，阻碍真正的转变，没有能挑战亚文化中的权力动态（“Notes on Survivor…”: 18）。

社群

施害者不仅要对受害者负责，更要对整个社群负责。对个人的虐待行为被视为对整个社群的伤害。施害者必须承担责任，在恢复团结之前不得重新参与行动主义项目。"对自身行为和社区负责，意味着承认错误并努力重建信任。这种信任超越伴侣或潜在约会对象的范畴，存在于朋友、室友、同志以及共同参与组织工作和行动主义的人群之间"（Crabb 2009）。其核心理念在于：整个社区都致力于实践预示性政治，并相互监督问责。

社群是施害者同意配合调查的主要原因。根据我的访谈，活动人士所在城市的规模会改变施害者的动机。在中等至小型城市中，人们无法在地理区域内更换社群。如果被威胁禁止参加某些活动或遭到特定人群排斥，实际上就等于被驱逐出社群了。亚文化与社会资本具有更大的影响力，如果资本更丰厚者不愿推进某项程序，该程序就无法实施。李曾在大学城参与社会活动，她说：

这类事件几乎总会演变成一场人气竞赛。究竟由谁来决定最终的叙事版本？由谁来书写这段历史叙事……几乎成了争夺历史话语权的斗争。当某人被点名批评时，随着时间的推移，幕后关于真实事件经过的流言蜚语会彻底改变人们的看法，进而影响他们是否需要致力于参与问责程序的感受。因此当某人被指责时，如果其本人社会资本匮乏，而掌握最多社会资本的人认为必须完成问责程序，那问责就会执行。反之，如果有权势的人认为被指责的行为是个玩笑，此事便会被当作玩笑处理。" 9:13

在李的经验中，文化资本和社交资本是决定某项进程能否启动并获得社区支持的关键因素。

在纽约等大城市，施害者可通过加入各种相互交织的亚文化圈子来逃避问责。亚文化资本和社交资本固然是因素，但权力更为分散 —— 仅仅是因为不同圈子里的人实在太多了。一位极具影响力的知名活动家曾被点名要求接受问责程序却直接予以拒绝。此后他被禁止参与多项活动及场所，相关传单被广泛散发，网站和博客文章如雨后春笋般涌现。十年后的今天，在相当一部分活动家群体中，他的名字仍与施害者身份紧密相连。

在各自社交网络中，同为活动家的伙伴们为幸存者和施害者分别组建了支持团队。对施害者而言，支持主要是普遍的道德支持，但绝不宽恕或合理化其行为。团队成员可能协助他们直面过往行为，并帮助满足幸存者的要求。"情感支持与无政府主义者开展的其他工作同等重要。除非我们保持稳定，否则无法成就任何事，而这需要他人的同情与支持”（莉莉丝）。这些支持团队可接管沟通事务，使幸存者无需与施害者直接接触。

幸存者决定向社区透露多少关于施暴者及其处理过程的信息。通常情况下，除非施暴者拒绝承担责任，否则相关信息不会被广泛公开。否则，信息通常会针对特定个人和群体。由于支持幸存者的前提是施暴信息公开，个人和整个社区都可能面临困难。如果幸存者不愿公开姓名或个人信息，就难以获得任何支持。例如在我积极参与期间，曾有起广为人知的争议性侵犯事件的处理。施害者姓名被公开，但幸存者身份没有被披露。约一周后，我收到友人邮件表示失望 —— 因我未主动联系提供帮助。当时我并不知晓对方正是受害者，也不清楚事件的全部影响。受害者身份的隐匿还意味着：即便知情者想告知他人，也可能因受害者要求保密而无法传达信息。

关于流程的传言屡见不鲜。闲话本身带有明显的性别歧视色彩和负面含义，但这种非正式的知识传播对活动人士却大有裨益，尤其在警示个人行为时：" '那家伙很猥琐，别和他来往'，到'我朋友被他坑过……'，再到'当心他私下很性别歧视'，最后变成'听说__性侵了某人，这是人们正在采取的措施……'"（Withers 2014: 51）。但情况可能变得复杂。我采访的一位受访者曾试图警告同城友人注意某人：

我曾向他居住的城镇的某人提起过，类似"此人存在同意权问题，提前告知"。我从未直接与他谈及此事，因为受他伤害的当事人并未授权我这么做。我不喜欢……我不喜欢说人坏话……但我不希望这人能随意出现在镇上……那只是私下低调的提醒……结果我收到这封信，写信人是我多年前的挚友，信中愤愤不平地要求我收回那番话…… 当时我不知所措—毕竟事隔数年，［受害者和我］早已断了联系。我绝不会去翻找她的联系方式打电话说："嗨，顺便提下，当年性侵你的那人给我写信了，我能告诉他你当时的感受吗？"不！我才不会这么做。绝不可能，所以我忽略了那封信。这很糟糕，因为我能设身处地想：如果哪天朋友突然对我说"嘿，有人告诉我你存在同意权问题，怎么回事..."...我会感到震惊、愤怒，简直糟透了。不过

我处理方式可能不同……天啊，我得向谁道歉才行？" 1:00:00

当然，流言蜚语也可能被用来传播关于任何一方的不实信息或负面信息，且在传播过程中很可能失真。关于幸存者"疯了"的流言相当普遍，对施害者行为的轻描淡写或夸大其词也同样常见。那些偏袒社会文化资本更高的活动家的流言，往往更容易被相信并进一步传播。

根据信息的清晰度、传播方式以及施害者与幸存者的身份，这可能导致社区成员感到必须选边站队。人们不愿听闻朋友、伴侣或同伴是施害者，往往试图将指控视为谣言、或为其开脱（Otto: 18）。某男性团体成员遭性侵指控时，成员们竟辩称"像他这样的好人绝不会做那种事"、或者"女人都赤身裸体躺在床上了，男人能怎么办？"（Dang: 9）。但否认等同于袖手旁观，本质上就是在纵容施害者。这种行为传递出"你更重视表面和谐而非他人安全"的信号（Accounting for Ourselves 2013）。

在某些情况下，施害者与幸存者的界定会受到质疑。施害者通常声称存在"相互虐待"，或宣称自己才是关系中的受害者。尽管亚文化群体中有人认同相互虐待确实存在，但这也属于施害者针对幸存者进行反向组织的一种形式。这种论调可能高度政治化，并给运动中其他人的关系带来压力。

转变性正义组织主张："当幸存者（即关系中弱势方）采取任何反击行为时，这永远属于自卫而非虐待"（Unowho）。然而，如果否定任何一方对事件的认知，将被视为社区指令，这标志着权力格局的重大转变。

例如在我对亚历山德拉的访谈中，就存在社区内部对事件产生不同解读的情况：

有人指控另一人性侵，仅此一桩。但某些人明白，在指控的另一面，存在着长期的情感虐待模式。而……我认为若当时我们有能力或勇气更明确地指出这一点 …… 或许结果会有所不同？但这很艰难，因为被指控者不愿采取以牙还牙的方式。就像'既然你

用'A'字开头的词，那我也用'A'字开头的词'。" 8:25

历经种种遭遇后，亚历山德拉认为"这种'永远相信幸存者'的理念……作为幸存者支持原则尚可理解，但作为社区问责原则则不然。"作为政策，将某个人视角和经历置于他人之上会使调解过程复杂化。

尽管有人主张当事人并非受审对象，但另一些人认为社群实质上扮演着陪审团的角色。"无需任何人受审，因为这里不涉及判决/裁决，且该机制刻意置于法律法庭之外……每位社区成员（即陪审团）将自主决定是否启动惩戒程序或予以忽视"（Vo 2011: 2）。在若干访谈中，活动家们以司法术语描述该场景。这种直接类比不仅未能体现新程序或替代程序的创造性，反而揭示了其再创造的本质。

社区也可能将问责程序引发的内部分裂归咎于幸存者。某些情况下，幸存者“被指责撕裂了社区，最终破坏了‘斗争’”（Betrayal 2012: 9）。问责程序可能加剧原有的个人与意识形态分歧，引发激烈冲突。发声行为会削弱幸存者的活动家公信力与文化资本。

[image]

问责流程

诉求

当幸存者明确界定虐待行为后，他们将决定施害者应如何向个人及社群承担责任 —— 具体方式因情境和关系差异而千差万别。幸存者的问责诉求取决于具体情况。在"费城挺身而出"项目中，幸存者通常会为施害者制定一份"要求清单"。如果幸存者有意制定要求清单，我们鼓励其思考：哪些措施能使其重获安全感与生活掌控权？哪些举措能使其确信施害者正为自身行为承担责任？（Colman 2009）

最常见的要求可能是要求施害者不要参加某项活动或进入特定场所，或协调安排使其避免同时出席同一活动。受害者通常不愿与曾伤害过自己的人共处同一空间。这一要求尤其具有争议性—— 在进入或处于

调解程序期间禁止特定人员参与，常被视为一种惩罚。有时这会成为施害者的绊脚石；"他们会因错过[活动]而心怀怨恨，或对调解初期未曾预见的种种牺牲感到不满"（Vo 2011: 2）。施害者可能被要求缺席活动，却不知晓指控者身份。在独立刊物节和书展等场合曾出现过争议性事件：施害者要求透明处理，而幸存者坚持匿名。在规模较小的圈子里，这种冲突更难化解 —— 活动数量有限意味着社交制裁的覆盖面更广。此外，我采访的几位当事人曾参与过这样的过程：幸存者要求施害者搬离共同居住的场所。

对幸存者而言，提出要求往往困难重重。如同涉及同意权的问题，即便心有不甘，他们仍可能承受着不就事件和场所提出要求的压力。幸存者一旦做出决定便无法改变主意（Withers 2014）。如果幸存者没有预料到施害者会出现在某处，仍可能被迫共处一室，或不得不亲自要求对方离开。在《转化性正义与伤害》中，A.J. Withers描述了自己演出时遭遇施虐者到场的经历：

"我记得当时说不能在他面前表演。我不断被问是否要求他离开。有次我表示不愿成为提出要求的人—总是被要求的是我，我不愿被单独指认……最终我还是说'好'。……但从团体角度看，当晚的'反派'竟成了我。好几个人告诉我，他们特意跨城赶来或取消其他安排只为看我演出。感觉大家觉得我反应过度、太敏感、像个大牌明星。本该有人关心我、体贴我，结果却怪我毁了他们的夜晚”（Withers 2014: 31）。

在某些情况下，活动组织者或其他社区成员认为幸存者“应该控制自己的情绪”，尽快走出阴影。这种默认不制定政策、不提出要求的状态，导致幸存者选择不参加活动，并逐渐远离某些场所。

协调活动日程对支持团体而言往往耗时费力。场地提供者和调解员有时也会被拉进这些对话。在访谈中，李女士坦言对那些要求幸存者避免出席活动或远离特定场所的沟通感到沮丧。

‟那种电话接龙的状况简直了！比如，谁来担任联络人……双方都有支持人员。那么这些直接支持人员是否也要负责接听电

话？幸存者想参加这场……激进诗歌朗诵会，想确认施害者是否出席。于是她联系协调人，协调人联系电话联络员，电话联络员再联系施害者的联络人，最后询问施害者是否出席。有时等整个流程走完，活动都过半了。” (Lee 1:11:25)

提出请求可能需要3至5通电话，施害者则会以另外3至5通电话回应。若出现分歧，或将场所问题纳入调解程序，沟通将变得更为复杂。

除调解和空间隔离外，请求可能包括归还物品、接受心理治疗、撰写道歉/责任声明书、告知新伴侣、支付医疗费用，以及寻求酗酒或吸毒治疗支持。其中接受心理治疗可能是最难实现的 —— 既能负担得起费用，又认同激进左翼政治理念的治疗师实属罕见。对部分幸存者而言，如果请求具体明确且迅速落实，调解程序或许无需启动。

分离

幸存者与施害者的康复过程通常是相互独立的。像"支持纽约"这样的转化性正义组织最初并未将两者视为独立流程，但随着时间推移发现，分头处理反而能取得更佳成效。分离流程还减少了双方直接沟通的频率，可通过支持团队进行协调。SNY制定了联络机制：由支持团体与调解团队指定联络人，"传达流程进展的总体印象，并将幸存者的反馈（包括对内容或阅读材料的建议）告知问责团队"（Support New York 7）。

不可避免地，在更具体的请求方面存在重叠。两种程序都可能依赖幸存者或施害者搬迁或归还物品。对于更笼统的"解决自身问题"的请求，幸存者与施害者往往对改变发生的时间表存在分歧，这可能导致幸存者遭遇挫折。实施转化性正义的团体会努力降低幸存者对施害者完全履行要求的期望，以减轻这种负面影响。

除此之外，幸存者的康复过程也是独立的。已有各类刊物作为指南记录这一过程，列出幸存者的步骤、可能的陷阱以及支持团队的建议。通常会向幸存者提供一份《幸存者权利与责任》清单。其中包含以下权利："有权对施害者感到愤怒、受伤、悲伤、爱或宽恕"、"有权讲述自身遭遇的虐待"、"有权直面施暴者及参与侵犯行为的人"、"有权去爱

和被爱"。责任则包括"照顾好自己"、"反思虐待经历对我的影响"、"建立健康关系"、"从过往的创伤、困境与侵害中幸存下来"（Lara 2011: 138）。

[image]

准备工作

在启动程序前，需要进行若干准备。如果现有问责小组没有承担此程序，则需要确定执行该程序的人员组。该小组必须制定接触施暴者的策略及问责方案。

“蝶蛹集体”在其刊物《美丽、艰难、强大：通过转化性正义终结性侵》中列出了8个步骤：

- 步骤1. 凝聚：组建幸存者支持团队
- 步骤2. 扩展：组建问责团队
- 步骤3. 沟通：界定团队间关系
- 步骤4. 储备与发展：制定转化性正义计划
- 步骤5. 召集行动：筹备首次接触
- 步骤6. 建立基础：首次会面
- 步骤7. 实现转变：与问责小组的系列会谈
- 步骤8. 评估总结：经验教训

某些团体在接触施害者前会先联络其亲友，以便受害者从一开始就获得支持（Quarrel 10）。这种准备工作所需的时间可能导致施害者提

前获知对质计划，从而开始组织反制行动或逃离当地。我采访的几位幸存者曾遭遇施害者提前获悉问责程序启动后迅速迁离的情况 —— 这种现象在亚文化圈中并不罕见。

在圈内更自然形成的程序通常较为非正式。小组构成可能不那么明确，例如可能仅由一人直接会见幸存者和施害者，或由幸存者团队担任调解人。另一种情况是施害者寻求外部资源，例如参加针对虐待伴侣男性的团体或匿名戒酒互助会。

调解人

有时，调解过程的调解人是问责小组的成员，例如纽约支持组织、费城挺身而出或女性左翼团体。对于缺乏经验或未加入问责小组的人士，通常会参考《站起来、行动起来》和《关于亲密暴力可能的社区回应的思考（再版）》等刊物作为指导手册。调解工作可由一人或少数人完成；但纽约支持小组发现三人协作分担任务最为理想。某成员在访谈中解释道：

"我们通常安排三名协调员进行问责流程，因为一对一过于亲密，几乎总是搞砸且怪异；两人一组很快就会陷入红脸白脸的套路...而三人似乎是神奇的数字 — 不同人会被不同事情激怒，所以...每次会谈中可能由不同人担任强硬派。"

由于施害者、幸存者、调解员及所有相关人员都属于活动家社群，团体内部可能产生人际矛盾。例如，我采访的一位活动家曾考虑担任调解员，而其伴侣正是受害者：

"现在回想起来，我简直不敢相信自己当时怎么想的！这个男人性侵了我的伴侣，毁了我们的关系。我居然要调解这种事？绝不！我恨透这家伙了……当时我愤怒至极，伤心欲绝。根本不可能以建设性方式 …… 但我觉得必须这么做，觉得有种女权主义的使命感逼着我压抑个人情感去完成正确之事。” 1:04:00

当关系动态从性和浪漫转向幸存者支持时，他们与伴侣的关系还是破裂了。我采访的两人还提到，有人自愿参与某个过程后，自己却被指控施虐。

由于这是自助式修复过程，参与者可能身兼数职。因此调解者必须承担相应的责任。在婕斯敏参与的一个案例中，幸存者选定的调解人似乎中途退出。幸存者要求施害者承担部分虐待相关的费用，但施害者"手握资金，而负责修复过程的团队中却没有人告知他该如何处理此事"。他声称'我不该联系[受害者]'（37:00）。结果该施害者'被多个空间封禁'，且人们基于他'未完成程序'的信息对他'做出诸多评判'（36:00）。

不一致是可以理解的，因为这项工作极具情感消耗性，且往往由幸存者承担。在访谈中，莉莉担忧这份心血可能对某些施害者毫无作用。"这要求太高了 …… 你知道，我认为投身这项工作的人往往本身就是幸存者……要求一群幸存者耗费时间去改造那些尚未真正愿意改变的人，这简直是种恶性循环。" 20:40. 亚历山德拉事后反思，从事这项工作时他们恐怕并非愉快的伙伴；"我在图书馆时突然意识到自己面容憔悴、神情阴郁……看着手边的书堆，竟发现有六本强奸和性侵相关的书籍里，还有一本奇幻小说！" 1:17:00

参与转化性正义组织的活动家们通过建立情感纽带，既缓解了与施害者共事的情感耗竭，也疗愈了自身遭受侵害的创伤。当我问及格蕾丝为何参与问责流程时，她回答道：

"那感觉既像是我想改变的东西，也像是一种开始的方式……就是和那些可能有相似的或略有不同经历的人待在一起，但他们都在谈论作为性侵、强奸或虐待幸存者的意义。通过这种方式寻找归属感—— 虽然当时不会这么说，但我其实在寻求疗愈途径：通过帮助他人、推动改变来治愈自己…… 以此应对并穿越那段令我深感无力的困境。"—— Grace 17:15

詹姆斯将年轻活动家在亚文化中组建集体的重要性置于特定语境下阐释：这既是他自我成长的关键环节，也是情感支持的源泉，更使他得

以理解并消化自身遭受侵犯的经历：

“我觉得我们当时都很迷茫，都很年轻，而且玩得很疯。有些人比其他人更甚……我真的不知道，如果没有每周的聚会，我是否能平安度过那段日子……我想当时我们谁也没有意识到我们彼此给予的支持有多么重要，但是……身处这样的群体对我在那个糟糕的世界里生存下来至关重要……我们通过与幸存者互助小组的聚会，学会了很多如何支持他人的方法，然后我们也用同样的方式互相帮助。在那段时间里，我突然意识到发生在我身上的事情是性侵犯，但我此前从未这样定义过它，这真的让我崩溃了。我记得我每周都在厨房里哭着向我最信任的朋友们倾诉，如果没有我们之间的那种情谊，我不知道自己该如何熬过那段日子。” 41:00

内部情感纽带也可能导致转化性正义团体的终结。在小众杂志《关于亲密暴力可能的社区回应的思考》第二版中，组织小组添加了附录：

“参与编写这本小册子的小组中有两位成员发生了争执（他们是室友），小组甚至无法讨论这场冲突。多年以后，我们彼此间已经不再是朋友。没有专家。这对每个人来说都很难。找到你自己的、更好的方法吧。” （3）

[image]

会面

如果定期会面，调解员和加害者通常每两周左右会面一次，整个过程理想情况下应控制在一年以内。根据他们的经验，纽约支持组织制定了一项政策，即“根据成员的空闲时间和能力”限制其开展的调解项目数量，并在公共场所举行会议（纽约支持组织）。他们还规定，只能与身处该地区或能够根据需要出行的人员开展调解工作。

此前曾流传着各种阅读清单和方法，但在2018年夏季，纽约支持组织（Support New York）最终确定并公开了其流程实施课程。该课程

将“身心实践和日记写作”融入阅读清单，以丰富其方法（Support New York 2018: 6）。该框架旨在灵活适应流程中不同需求和关注点的参与者。课程包含20个会议环节或主题，结合了学术文章和独立出版物，以及针对施害者的练习和作业。

例如，以下是第一部分第二节的节选：

第2节

讨论阅读材料及施害者的书面回应。该材料的价值在于规避了常见的"被诬陷"初始反应 —— 作者虽发现指控源于误会，仍强调需对社区负责。在此阶段，我们通常在挑战参与者与建立信任间寻求平衡，同时坚信参与者将在过程中成长。

活动

-《创意干预工具包》第4F节（承担责任）第1-7页
- 开始探讨该流程的初步步骤...
- 幸存者提出请求或要求，讨论需立即处理的事项（如安全顾虑、空间共享问题、沟通方式等）...

作业

反思幸存者的诉求（或社区请求，无论是表达出来的还是感知到的）与上述活动中所用工具包章节中提出的"责任作为过程与阶梯"理念之间的关联。可通过日记、绘画或清单形式完成。在此语境下，责任对你意味着什么？思考过程中涌现哪些情绪？

指定的阅读材料、写作任务及实践活动揭示了宏观与微观层面的性别动态。责任小组成员通过阅读和讨论性别歧视行为，尤其聚焦施暴者的行为及其自身遭受虐待和暴力的经历。

如果缺乏明确的议题框架和对话规划，整个进程极易陷入混乱。组织者凡妮莎·文德塔在《Ex Masculus》杂志撰文，讲述一位看似积极参与进程的朋友。她曾期待"施暴者能把握机会……但时间流逝，我从熟

识的成员口中反复听闻小组“从未讨论过任何实质内容"'（39）。同样在访谈中，李回忆起某次团队未能贯彻转化性正义实践的案例：

"...支援人员和我聊起'和那人的谈话进展如何？'，他却说'我不知道该聊什么。'我们只是过去闲聊。' '噢...我觉得你们该聊聊父权制和支配关系，或者...你觉得呢？'他却说：'我不知道该怎么和那人谈这些。我对他了解不够。' 天啊，这简直是失败。好吧。" 21:15

如果调解员对相关议题或调解流程缺乏经验，且对调解目的模糊不清，则任何形式的转变都无从谈起。

团队会议常促使施害者向幸存者或社区撰写信函，内容需包含"承认自身造成的伤害、阐述在此过程中获得的领悟，并明确未来改变行为的具体措施"（Support New York）。如果信函由幸存者提出要求，则可能专门写给对方。即使没有被要求，调解团队有时仍会以此评估进展。此类信函通常需经多次修改逐步完成，其最终定稿往往标志着整个过程的终结。

以下是应幸存者要求并经施害者同意，通过邮件发送给社区的责任信节选：

我的前伴侣不得不时刻提防自己言行是否会激怒我，从而危及她自身、我自身或双方的人身安全——尤其当她批评我时，因为我常在自我否定时情绪失控。这种压力迫使她背负着取悦我的重担。

肢体虐待在我们的关系初期就已存在，但在最后两年里，我的暴力行为不断升级……随着关系的持续，虐待程度日益加剧。

我持续：
砸毁她身边的物品，包括拳击粉碎卧室窗户
暴力掐住她
对她咆哮

扼住她的喉咙

我还：
殴打她
推搡绊倒她
将她推下楼梯

已完成流程的持续时间各不相同。在受访案例中，问责流程的周期从1个月到两年不等。其中一例流程持续超过一年，因为协调员与施害者之间发展成了更长期的导师/学员关系。提及流程较长的人士还提到人员日程安排、搬迁以及关系状况变化等因素。流程终结并无统一标准或决定性因素，许多情况下流程会自然终止或逐渐淡出。

[image]

第六章 发展与后果

> “我不认为这是场针对男人的战争。要真这么想，你家早就着火了。”—— 匿名作者，《她为何对你们的起义不屑一顾》

作为一种形式，问责制在行动主义亚文化中已实践至少十五年。从相关主题的杂志数量可见，转化性正义已成为处理性与虐待相关的人际问题的首选方式。由于与其他亚文化及机构的交叉参与，行动主义问责模式的变体已被应用于工会和音乐节。然而其争议性源于看似矛盾的特质：既严苛又散漫，既不一致又规范，既极端女权又父权，既过度热忱又冷漠，既激进又复制着国家或殖民结构。

活动家群体正积极拥抱这种追求正义与团结的方式。当"支持纽约"组织在某座缺乏社区问责机制的城市朋克音乐节上主持讨论时，一位男性身份者主动坦言，自己曾因某项如今看来是错误的行为而离开激进社群。他本希望当时存在这样的机制：既能为过错赎罪，又能留在群体中。即便在政策实施初期，部分活动家也迅速采纳了这些准则。数年前某次直接行动中爆发暴力冲突，一名有色人种女性受伤。施害者之一立即向社群邮件组发送声明，承认自身暴力行为、公开致歉并主

动要求承担责任。

但部分群体认为问责制过于极端，重构了警察与司法体系。无政府主义内部某些个人主义和起义派别反对将问责程序视为规范。我采访的几位人士认为，对流程的内部批判毫无空间。作为一种预示性实践，流程已固化为强制性规范，因而重构了权力结构，无法成为一种"解放性实践"（“Questioning Rape” 2014: 30 ）。

还有人对这项工作的局限性和社区成员的抵触情绪表示沮丧。尽管这些模式将幸存者置于核心位置，但有人认为"我们往往更注重帮助男性留在激进派圈子内，而非支持女性完成疗愈过程 —— 这可能需要将施害者逐出政治团体"（Nopper 2013）。据称女性安全常被牺牲，虐待行为仅因"ru 放任不管她可能不再为组织做'善事'"才被处理（Nopper 2013）。亦有观点认为某些情况下必须清除当事人。"当受害者因施害者将现身'街头派对'（即激进行动）而无法出席时，这难道算小题大做？如果我们直指问题根源，不顾'问责'原则直接终身禁入该施害者，这或许才是真正的激进派做法？"（Why She 2009）。

尽管转化性正义正被更广泛地采用，但女性和酷儿身份的活动家们离开社区的浪潮并未停止。当我和一位白人顺性别男性领袖谈及女性持续参与的问题时，他表达了担忧，希望她们不要全部离开，但他无法准确指出她们离去的缘由。"还有什么比女性和/或酷儿群体因屡遭欺骗、羞辱、身体/言语/情感/性虐待而离开运动更令人瘫痪？……没有什么比厌女者更能阻碍运动建设了"（Morris 2010）。

在下一章中，我将运用布迪厄的理论概念来探讨这些过程的结果。首先，我将考察权力动态以及社交资本在实施过程中的作用。社群如何看待幸存者、施暴者以及过程本身，都深受社交资本的影响。随后，我将分析文化资本如何与围绕暴力及国家存在的亚文化规范相联系。活动家的真实性与其是否愿意实施暴力并承受国家暴力打击密切相关。而来自社群内部的暴力则更具争议性。我将继续探讨社会运动的文化特质——实践如何植根于DIY伦理，以及这种伦理如何塑造实践的有效性。最后，我将审视这些主题对社会运动可持续性的启示。

[image]

社交资本与权力

谁能获得信任

社交资本源于知识地位或通过社交关系获取权力的途径。它决定了受害者或施害者谁会被相信，谁能获得社群的支持或辩护，以及问责程序是否启动。正如第五章所述，先锋反强奸男性团体"费城挺身而出"的大多数成员支持一名被指控性侵的男性成员，只因他是他们的朋友和共同组织者。

如同其他亚文化群体，女性、酷儿及非二元性别者，往往拥有较低的文化资本，其社会地位多依赖伴侣及其社交资本（Cohn and Mitchell 2015: 13）。在对贾斯敏的访谈中，她提及参与过这样一个案例：施暴者为一名跨性别女性，最终被迫离开了所在社群。

我认为她在组织工作和革命活动中具有不可替代的价值。但鉴于此事在更广泛的社会层面引发的连锁反应，她不得不选择退出。我真心认为这是运动的损失。她的缺席并不意味着运动中不存在更多客观上有害且更不负责任的人…… 这些人仅凭其特殊身份或圈内政治关系就拥有足够的社交资本，得以免于被驱逐。” 24:30

贾斯敏的朋友缺乏社交资本，实际上已被活动家社群排挤。其他犯下更严重过错的活动家仍能继续参与活动，而试图参与问责程序的人却再也无法融入这个群体。贾斯敏在访谈中指出，对跨性别者而言，在性别转换期间被社群驱逐或失去社群支持，会带来极度孤立感。李的经历同样表明，社交资本已成为决定性因素。

「就连我〝当面指责〞那次，其实也是邀请她来我家喝茶的，还带了个朋友陪着。我只是想说：〝嘿，我们之间发生了这事。对我来说真的很糟糕，我想让你知道。你能读读这些东西吗？我只是想让你明白事情的经过。〞 没有要求，甚至算不上正式的程序。

纯粹就是‵告诉你一声′。结果却演变成最混乱的局面。这种事你根本料想不到……她当时正和镇上社交资本最强的人交往，而我……我和他可是十年的老友！我完全没想到他会如此强硬地站队。但他确实这么做了，局面变得极其难堪。」41:20

在李的处境中，被指控者反过来指控李是施虐者。李最初试图通过相对低调、不那么公开的程序来解决，但最终演变成极具公众关注度的事件。尽管李与新伴侣是长期好友，但其前伴侣与新伴侣的关系性质赋予了前者特殊d 地位。由于新伴侣拥有庞大的社交资本，"施害者"的标签始终粘附在李身上—— 尽管他最初自认是受害者。

以幸存者为中心

将流程聚焦于幸存者可能给其增添额外的压力，将他们的转变与施害者挂钩，最终损害幸存者的康复进程。施害者标签的设立源于对改变的期许，但"幸存者"身份具有不可逆性 —— 这是无法脱离的角色，永远无法转变。幸存者身份是静态的。有人认为将自身视为幸存者并不健康或无益于疗愈，基于强奸或虐待经历形成的身份认同"在情感上并不健康……就个人而言，我认为将自己视为受害者或幸存者毫无助益"（"Half a dozen" 2014: 36）。

问责程序还给幸存者施加了揭露虐待的负担，迫使他们参与其中。这隐含着幸存者“有责任通过识别虐待并启动程序来阻止未来的虐待”。在《超越复仇与和解：击溃稻草人》一文中，作者A(legal)指出，当我们面对威权主义的刑事司法机构时，并不承担同样的负担。" 我们需警惕陷入传教士情结的陷阱：我们没有义务'拯救'或'改造'他人，尤其当我们与对方毫无关联时。我们不认为'感化'警察或法官值得付出努力，为何对惯犯就另当别论？"根据组织和支持团体的不同，幸存者还可能被要求组织整个程序。一位未加入既有组织的匿名幸存者表示："存在一种默认的期待，认为我应当召集小组。尤其是在召集小组这件事上，我承受了巨大压力 —— 这种压力直到后来我才完全意识到"（“Confronting Rape”）。幸存者可能被置于必须对施害者转变与行为负责的境地。

幸存者自动获得的信任，导致各方被简化为二元对立：幸存者被视为

善良正确，施害者则被认定为有过错且造成伤害。这种认知可能抹去了幸存者自身实施的伤害与压迫行为，包括种族主义、跨性别恐惧症、性别歧视和能力主义。对幸存者而言，一味的支持或许能带来慰藉并强化社群归属感，却无暇留给自我批判与行为改变，更无法在社群内部建立平等关系。当"善恶二元论"重现时，变革的初衷便轻易迷失。

在《Miklat Miklat》杂志中，一位匿名作者在《从虐待指控中疗愈》一文中讲述了被指责的经历。这位具有女性主义政治背景的跨性别者曾坚信"幸存者永远正确"，因而"主动承担了施害者的角色"。

> 我做了所有理应做的事来"承担责任"。但这丝毫没有改变他人对待我的方式—事实上，我的生活境遇和遭受的待遇反而变得更糟了。这让我觉得，许多高呼"社区问责"的人，其实并不相信施害者能够得到治愈，治愈也并非他们的真正目的...... 更令人不安的是，那些标榜倡导转化性正义的人，却会将你永远排斥并贴上污名的标签。那些曾为囚犯权利激烈抗争、向被控谋杀者寄送书籍的人，却毫不犹豫地排挤相识多年的我 ...... 很快，数百名素未谋面的人站出来抗议我在影片中的露面，暗示自己也曾遭我虐待，并坚称传播谣言是维护"社区安全"的必要手段。过去十年间，我努力克服了抑郁与愤怒...... 但这简直是噩梦。我好不容易建立的跨性别支持社群，转眼间化为乌有。电话不再响起，活动传单上赫然印着"禁止施虐者参与"—这分明就是在针对我。

当程序化处理成为常态时，那些可能不认同这些程序或不相信施害者能改变的活动家，仍必须以问责制作为解决人际问题和虐待行为的形式。而对于施害者而言，尽管"施害者"这一称谓旨在将虐待行为与个体分离，但这个标签在激进主义中却可能成为一种主导“身份” ——即便被贴上该标签后采取了任何行动，也很难摘掉这个身份。

拒绝参与和漠不关心

在某些情况下，施害者拒绝进入问责程序。施害者初期往往表现出防御姿态，否认事实、淡化虐待行为或归咎于幸存者。有时他们声称如

果不认识问责方成员，那就不属于同一社群，因此无需接受其“问责”。参与问责的核心动因在于社会契约 —— 个人为维持社群参与度和地位所作的投入。但这并非总是足够的。

施害者是否愿意承担责任，很大程度上取决于其留在社区的意愿以及社群对幸存者的支持力度。理想情况下，这个过程应被视为对所有相关方都有益。但正如当前政治环境所证明的，承担责任可能使当事人被认定并关联到不当行为中。在访谈中，亚历山德拉指出承认过错毫无益处：

"我们该如何回应他人，才能激励他们认同自身那些倾向于解放与蜕变的部分……并非说我们必须像哄小孩那样拍着头给奖励，仅仅因为他们做了最基本的人性要求—以尊重体面的态度待人，并对自身行为负责。但从集体层面而言，我们该如何建立社会规范来奖励负责任的行为与承担责任？因为现实情况是：当人们说'是的，我搞砸了。并公开承认错误"时，如果他们仍遭排斥、被视作污秽，这只会激励人们说："不，我没做过。不是真的。"这根本无法激励人们承担责任。" 39:50

正如第五章所述，参与该程序的唯一动力在于继续参与社群活动。但如果某人拥有足够的社交资本，即便无需承担责任，也可能持续参与。而参与该程序可能被视为承认过错。

即便施害者同意参与，也未必全心投入。他们是否真正"解决自身问题"，直接影响调解员的工作成效。纽约支援项目在培训课程中警示：如果施害者"未能以建设性的方式参与"，则不应继续投入精力维持流程框架。初期会议中常存在抵触情绪，但若至中期仍未克服（即目标达成率极低或相同问题反复出现），则应考虑转介至其他项目，或寻求施害者社区成员及朋友的额外支持（Support New York 2016: 9）。

施害者可能更专注于自我，通过自我受害的视角重写个人传记。在《Ex Masculus》杂志的《有你或无你：优先考虑同意权与构建更激进反文化的压力策略》一文中，瓦妮莎·文代塔谈及得知某位朋友强奸了另一位朋友的经历。瓦妮莎曾认为追责会奏效，因为施害者看似具

备自我认知；然而该过程最终未能成功。

他能够理解（在某种程度上），从幸存者在事件发生后立即与他谈论此事时得知，他的行为已构成强奸，并深深伤害了幸存者。尽管他承认当时并没有意识到自己的行为性质，但他并未否认，而且正与亲近的人坦诚地交流自己所做之事。他意识到自己对同意权的认知简直一塌糊涂，并表现出学习相关知识与技能的意愿……但随着时间推移，显然他并没能在任何方面采取令幸存者满意的行动……强奸事件后，他耗费大量时间谈论并沉溺于自身抑郁情绪、自我厌恶、经历的艰难处境，以及所有能缓解痛苦的诉求——这正是自我受害化与无助感的典型表现（40）。

尽管声称以幸存者为中心，但有人认为施害者才是整个流程的核心。他们能决定会面时间与频率，并获得一群人的关注。当聚焦于施害者的个体行为时，宏观层面的批判可能被忽视，整个流程反而可能助长自恋倾向。

当幸存者要求禁止某人出席活动或因逃避责任而被逐出特定空间时，处理流程往往引发激烈争议。安全空间通常禁止拒绝承担责任者进入。此外，幸存者或调解员可能联系活动组织者，告知某人正在逃避责任。关于禁令与沟通的概念常存在混淆。索菲亚在访谈中提及，某位担任领导职务的活动家曾询问团队是否要实施禁令。由于缺乏背景说明，团队自然表示不愿禁令任何人，认为所有人都应享有参与权。

"年轻时我参与某个活动团体……那时我大概19岁……还没听说过'安全空间'这个词……有人突然问我要不要禁止某些人参加活动，完全没说明背景，就这么问我要不要禁人。当时我才19岁嘛……当然回答'不要！为什么要禁止别人参加？"……后来有人向我解释了具体情况，我才彻底震惊了。我当时想，当然要禁止啊。原来如此，禁止他人是有理由的，但没有背景说明的话，我确实会感到困惑。所以后来我完全支持安全空间理念，人的安全至关重要。我时常回想起那段经历，真是次深刻的学习过程。" 40:10

经过几封邮件往来，她所在的团体被告知：被禁者要么是拒绝承担责任的施害者，要么是应幸存者要求不得出席的人，同时实施了安全空间政策。

在某些情况下，当组织者不愿或无法制定政策时，幸存者及其支持者会尝试直接要求当事人离开，这往往会引发冲突。在《我们该怎么办？》第三期杂志中，一位匿名作者描述了这样的场景："你竟为自己留在场内的权利辩解，而其他人坐在外面流泪，还有人直接离开了聚会"（第3页）。

复仇与权力

当幸存者揭露施害者时，他们或许正试图从施害者手中夺回失去的权力。但行使社群权力的问题错综复杂，而责任追究的言辞往往回避了复仇与报复的讨论。在《安全不过是幻觉》这篇最具影响力的对问责制的批判文章中，奥古斯蒂亚·塞莱斯特主张我们必须去本质化"幸存者"这一类别，并在亚文化中更直接地追求正义。"如果有人伤害你而你想报复，那就去做，但别假装这是为了共同疗愈。权力交换就该直呼其名。渴望夺回权力无可厚非，主动夺取亦无不可，但切莫对他人施加任何你无法忍受的报复——当角色互换时你自己也无法承受的那种事，不要做"（2014）。受访者玛丽认为，她参与的某个过程更像是复仇而非追责。她表示："对刚经历性侵的人来说，复仇作为即时反应可以理解，但这对双方的康复都无益处。"

权力差异在"反组织行为"中尤为复杂。反组织行为被视为针对幸存者的恶意行动。通常，反组织行为指被指控施害者主动组织力量对抗幸存者，例如宣称对方精神异常、关系中存在双向虐待，或声称自己才是关系中的受害者。转化性正义组织主张："当幸存者（即关系中权力较弱的一方）以任何形式反击时，这永远是自卫而非虐待"（Unowho）。

公开谴责

如果施害者拒绝承担责任或处理过程未获成功，其行为可能遭到公开谴责。如前所述，当受害者希望保持匿名，或公开施害者身份必然暴

露受害者时，此举将面临困难。在亚文化圈内，存在两种传统的公开谴责形式。第一种是向社区公开的信函或声明。此类文书会通过邮件发送给个人及团体，或在活动中印刷分发。近年更常见的是将揭露信张贴于Indymedia、Facebook及相关组织网站等平台。

第二种形式是通过地下刊物。最早且最著名的案例之一是《宝贝，我是大男子主义无政府主义者》。它开创了利用地下刊物 —— 这种在无政府主义文化中最为普遍的传播形式 —— 向社群揭露施害者的先河。该刊物揭露了某位社区活动家长期虐待多名女性却拒不承认行为的事实。一位幸存者联合数名支持者共同制作了这本杂志，旨在向其他活动家揭露她们在遭受虐待期间及事后与该男子的经历与互动。

最著名的公开谴责案例之一，便是以激进团体为核心，同时运用公开声明与独立刊物展开的抗争。一对夫妻共同创立出版团体后，在激烈离婚纠纷中企业资产被丈夫独占。该女性公开揭露丈夫的虐待与操控行为。虽曾尝试一两次问责程序但均告失败，活动人士试图推动出版集体制定安全空间政策并追究该男子的责任。女方在小册子中撰文描述婚姻经历，男方则以小册子文章反驳，指责问责程序存在健全主义歧视的倾向。在多份公开声明及往来信件中，该集体时而否认、时而承认、时而坦承过错。部分集体成员已退出，多位作者停止与该集体合作出版。

由于所有这些互动都植根于预示性政治，公开此类信息存在矛盾。尽管活动家生活方式中的性积极文化实践已打破这种界限，但仍有部分人坚持将浪漫关系与性关系与公共生活割裂开的传统观念。此外，仍存在"认为遭受系统性压迫的群体（如酷儿群体和有色人种）不应'公开内部暴力'的观念，因其可能被利用来进一步妖魔化这些群体"（Accounting for Ourselves 2013）。在访谈中，有两人明确表示“后悔”发表公开声明，主要原因在于遭遇同侪活动家的强烈社交反弹，且此举未能有效遏止当下或未来的伤害。

我当时感到不知所措，完全不知该如何应对。现在想来，发布那封公开信简直是……最愚蠢的决定，我当时能做的最蠢的事……不过事后看来，这或许还不是最糟的，因为它引发了这场公开信大战 — 现在回想起来，我心想"当然啦，他们肯定会回击的"。但当时不知为何觉得他们不会这么做？真不知道自己当时在想什么。”

Lee 46:00

"我让愤怒主导了决策。这显然不是正确选择。后来我写了一封公开信给社区，并散发了出去……我表达了我对这个人的不满，我认为……多年后，什么都没有改变。" Mary 53:52

[image]

文化资本与暴力

预防与恐惧

随着问责机制的日益普及，部分活动人士坦言担忧遭受指责。这种恐惧正限制着他们的性关系、社区归属感，甚至可能阻碍其参与社会运动。偶有文章如《为何我开始畏惧社会正义运动中的同伴》指出："目睹无数人因过失在社群中遭到无情的撕裂后，我开始畏惧自己的战友"（Lee 2017）。同样地，在经历几次负面审查后，贾斯敏对活动家运用转化性正义的方式产生了高度警惕，尤其担忧这种做法对那些将社区视为替代家庭的人群造成的深远影响。

“我认为对任何运动而言，人们对犯错感到该死的恐惧都绝非好事…… 那种感觉就像，一旦失足就会失去所有社会支持，沦为彻底孤立的酷儿，连刚才还称之为社群或家人的那些人都会离你而去。” 42:30

另一位受访者曾撰写过一本批评问责制的热门杂志。他们告诉我，有位读者来信说自己的朋友在被公开指责后自杀了。

有人认为不应惧怕被揭露，而应将其视为审视自身预示性政治理念的契机。《我们都是幸存者，我们都是施害者》小册子指出："此过程旨在让施害者理解，'被揭露'并非惩罚，而是馈赠。这是成长的契机。拥抱这个过程。施害是懦弱的，坦白才是勇敢的”（2005年）。然而，尽管预示性政治需要自我反思、自我批判和自我转变，这些行为仍未

完全被接纳或获得积极评价。

另一些人则认为这种恐惧是女性所经历恐惧的对应物。"也许这是你人生中第一次体会到走进房间时，无法自动判断是否安全，无法辨别谁是朋友的感觉……我没时间同情你，绝无可能，更没有时间—当美国每两分钟就有一名女性遭强奸时…… 我没空抚慰你受伤的自尊，更不会为垂死的父权制流泪”（Anxiety 2004）。同样，我采访的一位人士指出，尽管女性在问责制中可能掌握大量权力，但这或许是权力天平的摆动—这种权力动态的转变，或许正迈向更具社会正义的人际关系。

文化规范与暴力

激进左翼亚文化圈的大部分活动都围绕着深夜派对展开，这些场合常伴有酒精及其他物质。正如第四章所述，亚文化圈还倡导性解放理念，随意性关系十分普遍。其结果是，性行为的同意往往无法确立或难以明确。

尽管存在关于同意权的研讨会，但它们很少触及药物使用问题。这部分源于酒精使用相关的广泛文化规范。"幽默和交谈规范强化了这样一种观念：极度醉酒是正常且有趣的，人们醉酒时的行为比清醒时更不负责任。周末接连不断地，我们营造出高度性化的空间，伴随着强烈的酗酒压力，导致人群酗酒或吸毒过度，无法给予或接受明确的同意。"（Accounting for Ourselves 2013）。那些被标榜为"安全空间"的场所往往缺乏系统性防范机制，仅依靠零散的非正式监管。我与朋友们曾数次护送女性回家，或主动询问那些看似丧失同意能力的人。

围绕问责程序的另一项文化规范是非暴力原则。该亚文化群体在行动策略上绝非反暴力，但在处理人际问题时，强烈反对以暴力作为报复手段。在程序之外，确实存在幸存者希望对施害者实施身体报复和暴力行为的情况，例如殴打对方。"是采取本能的肢体反应——甚至复仇——更诚实、更直接、更真实？还是参与冗长的伪司法'程序'？（“Notes on Survivor Autonomy” 18）"

曾发生过几起引人注目的事件，幸存者及其支持者对施暴者实施了人身伤害。正如历史小册子《我们村的锤子》所记载的："自2010年起，部分女权主义者摒弃了问责策略，将锤子挥向了相反的方向；她们转向了私刑复仇"（第20页）。以下节选自采用此策略的团体发布的匿名声明，这些声明被其他小册子转载。我已删除具体名称，但原始声明及小册子副本中均有记载。

"此人惯用反父权术语，早有性暴力前科，并曾参与幸存者主导的问责程序。鉴于其持续越界，在波士顿和圣克鲁兹对女性实施强奸和性侵，我们决定当面质问。我们前往其住所进行言语交锋，他拒不承担责任，言辞充满操纵与侮辱。当他拒绝闭嘴时，我们让他闭嘴了。此举意在施加痛苦，尽管这仅是其受害者承受痛苦的冰山一角……某些自称'男性盟友'者试图通过自行解决、施压要求女性参与、未经许可召集公开会议等方式掌控行动，这破坏了我们的自主组织实践。这些男性非但未表支持，反而明确表明不愿让我们在没有他们参与的情况下自主行动。我们作为女性身体的同志群体所采取的行动，显然符合反等级政治和自我决定的目标。如果男性身体的"同志"们希望被视为同志，我们希望看到他们以相称的方式行事…… 此次行动开创了先例，标志着新型问责机制的启动 —— 它既让施暴者承受痛苦，更昭示着我们对激进政治社群乃至更广阔领域中男性霸权的彻底清算。我们深知****并非唯一罪魁祸首，世间还有更多同类存在 …… —— 匿名组织声明

"凌晨三点，他在……小屋里被喧嚣声惊醒。十三个人影围住他，多数戴着面具。被他强奸过的女人将一杯经血泼在他头上。她掌控着后续行动，在群体力量的庇护下，毫无畏惧地直面强奸犯。这场诗歌朗诵会交织着强奸与反抗的主题。我们轮流倾诉愤怒，诉说伤痛，最后表达对他康复的期许。当他辩称强奸并非暴力行为时，她一拳击中他的面颊。我们刻意避开白昼实施行动，只为让他心生恐惧。我们让他体会那种在黑暗中赤身裸体、毫无防备的无助感。我们行动，更因我们绝不容忍强奸作为社区的常态"—— An Internal Action by the Vaginal Liberation Front

"至少，施暴者应该有所触动，他的行为应该留下某种持久的印记，让他每次发生性行为时都铭记于心——当然，前提是他还能再有性行

为。所以我们决定确保这次侵犯成为他永远忘不了的经历。我们带着棒球棍闯了进去。我们把他的书从书架上扯下来：他承认了，没有一本书提到过同意。我们逼他喊出：'我是强奸犯'。我们把他丢在黑暗的床铺上一个人哭 —他再也无法在此获得安全感了。这是先例。这是新型问责机制的开端，让施害者承受痛苦— 尽管这仍只是他造成伤害的冰山一角。我们知道*****并非唯一的罪人。我们知道你们还有更多同伙。我们毫不后悔，也绝不停止：从今往后，我们将以暴力回应性暴力。"— ” We’ll Show You Crazy Bitches II

这三起事件均涉及女性及非二元性别者对性侵者或其朋友实施的暴力报复。这些公开事件既是对涉事者的当众谴责，也对司法程序构成了批判，同时要求赋予暴力行为以政治正当性。此类行为在参与者间形成团结纽带，其直接性颠覆了女性及非二元性别者"非暴力"的刻板印象。

上述这三份声明中的最后一份发生在我参与当地激进主义亚文化期间。此事声名远播，以至于在我的访谈中，一位中西部活动家提到这个故事时说："就是有人抓到施害者，用棒球棍揍了他一顿，大家都为此兴奋不已。" 尽管旁观者或许为此振奋，但参与其中的女性、酷儿群体及非二元性别者却遭遇社区内部分人士的强烈反弹，甚至面临人身暴力威胁。最知名的参与者遭到了"人肉搜索"—— 他们的住址等私人信息被公布在无政府主义社群的邮件列表上，而警方无疑正密切关注着这个平台。

尽管大多数转化性正义组织反对使用肢体暴力，但最终由幸存者决定如何处置施害者。"如果她们希望施暴者接受街头正义的惩罚，这也是她们的选择。只需给予支持，切勿妄下结论"（Said the Pot）。有人认为女性可以实施报复性暴力，而男性则不可，因为他们必须"打破男性暴力的循环"（supporting a survivor of sexual assault）。另有人主张，此类暴力仅应作为对身体暴力行为的报复手段（“Half a Dozen” 2014: 38）。在四次访谈中，当暴力议题被提及时，受访者均表示担忧此举可能适得其反，反而对幸存者造成进一步的伤害。

反情报计划、警察管制与国家机器

反对这些政策的人常将相关行动与警察国家相提并论，以此剥夺其正当性。尤其在某些无政府主义群体中，任何行为规范都被视为反革命。当访谈中提及"警察式监管"的问责制时，各方反应不一。

"这本质上就是社区警务。你们在暗示对亲密性关系及人际交往存在既定行为规范，一旦有人偏离这些预期就会面临后果。从定义上讲，这正是你们在做的事。虽然你们运用权力的方式可能不同于国家机器，但你们通过声誉、社区空间准入权、社交资本来施加影响力。我认为这种类比成立，因为他们深谙此道。"（Willow）

‟我他妈觉得这主意蠢透了……蠢得连理由都明摆着。而且根本不现实。人要共处一地，即便我们要在人间建立心中理想的新世界，仍会有怨愤需要化解。革命绝非人人为所欲为—那不是我理解的无政府主义。”James 33:05

我能理解这种观点……问责制……本质上是对社区伤害的集体回应，尤其针对个体伤害。但任何针对伤害的集体回应难道不都叫作监管吗？……这需要更细致的区分。我的意思是，我们不会把人交给警察，所以绝大多数时候都在规避司法系统，因此这并非与警方合作，谢天谢地。但我也能理解，其中存在一股个人主义自由倾向—尤其在那些更偏向自由意志主义的无政府主义者中，他们淡化社会维度，主张他人无权干涉个人选择，每个人都该为自己负责……那么任何发号施令者都会被视为警察。我认为他们确有某种薄弱却具哲学意义的论点，只是忽略了人类相互依存的本质。"Carl 53:35

被审查的对象可不只是性取向。各种各样的事情都在被审查。所以我不希望人们……当我听到所谓的问责制其实是彼此监督时，有时会忍不住发笑。因为我在想："天啊！这些小圈子简直事无巨细地互相监督！从衣着打扮到用词选择，从阅读书籍到言行举止……我们不仅在监管彼此的性取向，更在监管彼此生活的方方面面。我并非认为这种监管永远是坏事……但多数时候它确实糟糕透顶。我内心反复纠结：人类渴望相互契合是否本质上错误？有时强迫他人效仿自己确实荒谬至极，但当涉及性别代词这类议题时，我又会想：‵等等！我确实希望所有人都这么做。′” Lee 54:00

正如这些引文所示，对于将该实践类比为“警察行为”及其正当性的判

断，存在着多种观点。个人自由与集体融洽之间的平衡被置于对立面了。此外，将"警察式管理"应用于性关系、社交互动或整体文化的议题，也引发了讨论。

尽管警察和国家司法机构通常被视为负面存在，但其核心理念却深深植根于我们的正义认知中。初次接触转化性正义理念时，很难想象一个不遵循"未经审判不得定罪"原则、不考虑惩罚形式之外的请求或诉求、且无需定罪的司法程序。正如《自我清算》作者所指出的，就连"反国家武装分子"也会提出这样的质疑："无罪推定原则去哪儿了？我难道不能获得公正审判吗？不能为自己辩护？请听听我的品格证人的证词啊！"

COINTELPRO，即上文提及的1950至1970年代政府反情报计划，曾用于渗透并瓦解政治组织，如今常被指在社区司法模式中死灰复燃。参与者被质疑“内讧” - 从内部瓦解阵营，可能充当政府工具。这些指控使社区司法的激进性受到质疑，并暗示存在某种程度的"告密"行为。在访谈中，伊娃阐述了COINTELPRO如何被用于削弱问责机制的正当性：

"它立刻让人联想到告密、当线人、搞阴暗勾当，还有破坏行动。就像这是种排斥他人的方式，就像在说'他们可能是线人，这全是COINTELPRO的把戏'。COINTELPRO成了'此人不可信'的代名词。
他们所言皆虚，只需声称'这是政府派来的破坏者'就能否定其合法抗争'......
并非说线人不存在——确实存在......但政府线人往往主动制造暴力冲突，迫使人们应对暴力局面。问题不在于有人煽动暴力，而在于施暴者本身就是政府线人......或者他们能利用本就存在的紧张关系。” 59

[image]

返回：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

许多自认女性和酷儿身份的人士辩称，他们并非在实施监管，而是自身自由已然受到侵犯。存在着一种"不幸的矛盾：既渴望不受他人规则

或强加束缚的生活，却又不愿面对他人遭受压迫 —— 因为这意味着你追求某种自由的努力将被中断"（Thunder Collective）。当涉及群体行为时，限制与规则实属必要。对女性与酷儿群体而言，安全机制反而具有解放意义——正如《为何是她》2009年所言："这意味着挣脱彻底的社会政治操控枷锁，为集体自由而战，摆脱性别与性别认同带来的压迫与期待。”

与此同时，依赖社区正义而非警方的做法，可能被用来对付幸存者。有几位知名活动人士曾被"点名批评"却未被追究责任，反而试图起诉各自的幸存者。在政府眼中，这些行为既无官方记录也缺乏虐待证据。《争吵》杂志明确声明："我们希望保护我们的成员免受警方执法，如果某些目标对象对我们及/或幸存者提起法律诉讼的话。告密者必遭报应。xoxo"（《争吵》第6期）。迄今为止，其中最受关注的案件已被驳回。另存在若干案例：被揭露施虐行为的男性身份活动家虽未因性别歧视行为受责，但当其动用国家暴力（警察）对付同侪时，最终被驱逐出社区。

[image]

实践和成效

DIY流程

流程的DIY特性既意味着社区具备执行此类工作的能力，也体现了其肩负的政治与道德使命。流程信息通过互动交流和小册子的传播，但这种方式未必始终连贯高效。重点在于亲力亲为获取第一手经验，并分享这些经验和技能以助他人。在访谈中，伊娃表达了对某知名学者就"占领华尔街"运动中人际暴力与性别暴力问题提供咨询时所表现出的态度感到失望。

变革需要人人参与。每个人都有能力参与这项工作…… 即使你并非专业人士，也具备相应的技能…… 我认为人们应当始终尊重学位认证，尊重特定经验……当我首次在阅读著作或听她演讲之外与朱迪斯·巴特勒接触时，经历了令人失望的'偶像崩溃'时刻……虽

然依然对她怀有崇高敬意，但当时人们竟要求她对'如何应对占领运动中的暴力'这类她完全不熟悉的领域发表权威见解。她的回答很糟糕……最后有人问她关于安全空间和社区协议之类的问题。她只是敷衍道"是啊，很难"，然后抛出一个方案：设立专门的"观察员"，让他们站在外围观察、审视来者。但这就演变成了：我们究竟要赋予哪些人权力来决定谁能来谁能留？类似的问题。简直糟透了，你不过是在重构那些操纵性、压迫性的结构……我当时还想：朱迪斯·巴特勒，你凭什么对这事发表意见？1:36:00 Eva

即便在"占领运动"群体内部，专家意见也备受重视。伊娃感到沮丧，因为她在参与运动前就对安全空间政策有切身体验，但人们却显然更加重视朱迪斯·巴特勒的观点——尽管这位知名学者既没有直接经验，也并不专攻此领域。巴特勒对该问题的回应在政治立场上既不激进，也未见深思熟虑，而这些正是伊娃这类人士反复斟酌过的议题。

我采访的其他活动家认为调解工作需要专业资质，他们在寻求专业流程协助时也遭遇了困难。

我也好奇……假设一个文化群体极度崇尚DIY精神，凡事都要自己动手解决，这种做法究竟能有多大成效。毕竟有专业人士撰写书籍、开展培训，专门指导修复性司法流程等事务，而参与这些问责程序的人员中，多数人并不具备相关经验。我认为他们更多是出于个人动机，而非真正具备资质。这本身未必是坏事，但在涉及强奸或殴打这类严重事件时，问题就显而易见了……专业治疗师需要多年研习才能掌握干预技巧和非暴力工作方法。仅凭参加活动或表现出强烈关切，显然不足以让你具备解决如此重大社会问题的资质。”——Mary 25:15

玛丽认为这些问题过于复杂，不应由缺乏经验的人来处理。虽然她认同需要专家介入，但强调这些专家必须是特定领域及心理健康领域的专业人士。寻找专家的困难在心理健康和外部援助领域尤为突出——既要找到价格合理、政治立场相近的治疗师或咨询师，又难以兼顾专业资质。围绕反等级制组织、性别认同、虐待定义及权力动态的激进政治理念，未必与传统心理健康专业相契合。此外，并非所有活动家

都享有医疗保险，即便有保险，也可能无力承担共付额。

独立刊物的DIY形式在阐述问责机制时缺乏一致性。不同刊物提出不同主张，将某些步骤描述得看似简单易行，实则操作困难，且可能仅适用于特定情境或城市。莉莉在访谈中坦言，她最大的遗憾在于曾撰写刊物将问责流程描绘得过于简单直接。

"某种程度上，我后悔的并非流程本身，而是关于问责制的那些文字。我后悔让它看起来像是能够真正实现问责、治愈社区的途径。我的文字助长了这种理想化的想象，而现实中要有效运作，需要社区更强的凝聚力，参与者更深的奉献精神和专业技能——是的，我为此感到遗憾。我后悔让它看起来比实际更容易实现——尤其对普通人而言。我认为开展这种心理工作需要特殊技能和专业训练。" 17:07

在多次访谈中，受访者表示事后回想，他们实施的流程显得笨拙或混乱。部分原因在于组织混乱、未能预见反应、相关议题引发的情绪动荡，或是缺乏长期规划。

"我主持过一次会议，简直是一场灾难……现场气氛异常紧张，所有人都情绪激动。房间里充斥着强烈的情绪波动，我认为这模糊了判断。"—— Mary 15:45

"现在回想起来，我只能感叹'有些场面简直乱成一团！'"—— Lee 45:30

"总体而言，我们已在极端困境中竭尽全力——所有人技能严重退化，初始环境就充满创伤，性话题等诸多禁忌与矛盾又相互交织。能完成任何工作都堪称奇迹。" —— Alexandra 7:30

作为一项自发实践，参与调解的人员必须平衡工作与生活中的其他责任，包括工作和学业。这项工作由社交活跃的年轻人承担，可能带来巨大的情感消耗。仅有一位受访者提及个人吸毒或酗酒行为影响了工作。

"我记得有段时间自己压力非常大，根本无力做好任何事，因为整个人都糟透了。有段时间我每晚都泡在酒吧直到打烊，和老板在吧台上吸可卡因。睡到下午四五点，做些狗屁工作……勉强维持生计，同时还要主持三个问责程序。这简直荒谬至极。我想这正是人性弱点——当无法自救时，便试图拯救他人来逃避面对自身困境。回望那些时刻，我虽未在任何流程中表现糟糕，但完全处于自动驾驶状态。而这类工作本需要深度投入。" James 37:00

其他人则谈到睡眠障碍、沟通不畅和难以协调的日程安排。在《变革始于家庭》一书的章节《当变革终于到来时是什么感觉》中，RJ·马卡尼描述了他尝试组织问责小组的经历。

"这个小组耗时一年多才真正成型：X先生在多方面拖延，而我们其他人则在处理多重事务的同时努力推进这个进程。耗时逾年才将丹妮尔和我（两位最初站出来指控的女性之一）、X先生，以及另外五位与X先生存在关联的人（包括现任或前任朋友、关切此事的社区成员）同时召集到同一房间。" (Jashnani, Maccani, and Greig 2011: 222)

在后一种情况下，该流程采用圆桌会议形式：召开一次长时间会议，通过讨论形成诉求清单，部分参与者承诺协助并跟进施暴者对诉求的落实情况。但在人口流动性强的亚文化群体中，为处理暴力或虐待事件进行长达一年的前期准备工作，时间跨度实在过长。

转化性正义所需的工作体现了传统的性别分工。尽管部分团体自行维护安全空间，但仍有集体组织协助实施相关政策。这些集体成员主要为女性或酷儿身份者。工作内容包括：制作标识牌及其他空间标记物、召开战术会议、编制禁止出席人员名单及潜在问题清单、保持清醒并全程保持警觉，以及实际执行政策。

在施虐者与幸存者的转化性正义工作中，同样存在这种分工现象。虽然有少数男性团体参与具体个案，但大部分工作仍由女性或酷儿身份者承担。具体工作包括：设计阅读课程、每周与施暴者进行数小时面

谈、定期与集体或更大工作组开会沟通、随时待命接听电话、有时需暂停所有事务赶赴现场处理突发问题、承受与施暴者共事的情感压力，以及举办工作坊引导他人参与。普遍共识是"处理这些烂摊子的人绝大多数是女性"（Why She 2009）。这种分工令人沮丧，活动家们呼吁需要更多男性盟友。如今许多女性和酷儿群体被要求付出双倍努力，既要在政治场域提供情感关怀，又要在个人空间承担情感劳动——而这些私人领域至今依然存在（Mitchell 2016: 15）。

官僚主义

对问责制的诸多批评还在于，这种调解机制增加了不必要的官僚程序，消解了直接对抗的可能性。在前述《安全不过是幻觉》一文中，奥古斯蒂亚·塞莱斯特指出活动家们"建立的模式鼓励各方仅仅通过谈判来确保永远不必再见面或共享空间"（2014）。《我们村的锤子》女性主义杂志指出，当组织者耗费时间处理内部矛盾时，"如果每次两人不合就扰乱政治环境，我们就不再将政治工作置于首位来。我们退化成朋友圈、性俱乐部或互助小组。这类团体未必优于政治项目，但本质截然不同」（16）。有观点认为小型调解机制或许能「避免冲突升级，节省本该用于其他优先事项的团体精力」(A)legal),，但其他活动家仍持更悲观态度。

定义“成功”

部分女性主义活动家也质疑转化性正义在应对性别暴力方面的有效性。“成功”并无固定标准，参与者对其定义各异。如果某项程序旨在"搞定这个烂摊子"，这意味着当事人必须完成哪些事项？何时方能宣告完成？如果目标是预防未来侵害，那么成功是否意味着已杜绝进一步伤害？如果程序以幸存者为中心，是否应由幸存者来定义“成功”？与监狱制度讨论相呼应的是，问责制究竟旨在威慑、改造还是保护社会，其目的仍不明确。此外，一个新问题随之浮现：作为认同社区革命政治理念的同志，施暴者是否应适用较低标准？抑或因其存在有问题的行为，抑或因其政治觉悟水平从而需要更高的标准？

经历一个过程并不能保证实际行为改变或全面转变。有人担忧施害者——他们常被指控操纵他人——能够利用问责话语为调解团队制造看似理想的结果。在《转化性正义或成伤害》中，A.J.威瑟斯指出 "人们

担忧……造成伤害的个体只是表演问责/责任，而非真正履行"（2014:36）。新的亚文化实践可能为操纵性和伤害性行为开辟新空间。部分独立刊物揭露施害者利用问责程序施加权力或延续与幸存者的互动（Withers 2014）。施害者在程序结束后是否改变行为仍存疑。

如果一个程序是以幸存者为中心的，那么成功与否似乎理应由幸存者来决定。总体而言，幸存者似乎认为，只要请求具体明确且能立即得到处理，程序就是成功的。露比是我接触过的唯一明确表示过程成功的幸存者。尽管她不确定施暴者是否改变，但要求对方搬离共同居住环境的诉求得到了迅速响应。然而对某些幸存者而言，即便施暴者完全履行了所有要求，他们仍可能认为对方并未真正改变或转变。

当我询问作为协调员或调解员参与过程的人员关于成功案例时，结果呈现出复杂的局面。

我认为成功率在七成到八成之间。所谓成功取决于衡量标准：如果成功指幸存者原谅施暴者，那么成功率约为一成；如果成功指幸存者获得了必要的疗愈空间，且施暴者表面上—至少据我所知—没有再延续虐待模式，那么成功率就高得多。据我所知，完成整个疗愈过程后仍继续施暴行为的人 ……仅有一两位。"—James 35:25

我认为……大多数疗愈过程都取得了显著成效……但我实在无法说清有多少幸存者在疗愈过程中……认为疗愈本身是成功的…… 衡量成效确实是个难题，而且我不知道……这些流程缺乏标准化的后续机制……我们掌握的案例数据往往令幸存者感到挫败—要么是诉求未获满足，要么是因流程拖沓冗长、最终草草收场，未能以令人信服的方式达成实质性成果……"— Grace 28:35

"其中我认为有一次非常成功。另外三次虽有成功时刻，但总体而言…… 如果以'成功'定义为：幸存者感到诉求得到满足且获得疗愈空间；施害者完成深刻自我反思并承诺不再造成伤害（至少不再造成同类伤害）；社区整体得以维系或从创伤中康复……这四次案例中仅有一次达成此标准…… 上述三项要素既是成功的充分条件也是必要条件……其余三例虽具备部分要素，但总缺失关键一环。"李 35:30

这些引述表明，二元化的成败分类无法契合实际进程的体验。尤其当以幸存者为中心的过程未能达成以幸存者为中心的结局时，这种矛盾尤为突出。

[image]

社群与可持续性

其实并没有社区

问责制建立在社群理念之上。社群是最终对个人进行问责的主体，相关流程植根于行动主义文化。这种预示性问责政治融合了个人与政治、公共与私密。部分行动者对此提出批评：行动者社群并非真正意义上的社区，预示政治具有封闭性，不利于群众运动的建设，且流程术语的使用会通过政治话语疏离个人体验（Cohn and Mitchell 2015, Celeste 2014）。

该模式源于原住民社区的实践经验。参与转化性正义的活动家常援引纪录片《Hollow Water》，该片讲述加拿大某原住民小社区应对儿童性侵疫情的故事。但正如我在若干访谈中指出的，这跟我们的社群背景存在差异。 BACK [image]是否有比米兔更好的解决方案？如何？：超越米兔S09E01

我们谈论社区问责制……但现实中我们并不真正拥有这样的社区……我们受到《Hollow Water》的启发……而他们生活在孤立的社区里，人与人之间都彼此相识或有亲属关系，因此存在着不同类型的社会压力。而我们并不生活在这样的环境中。我们目睹施害者离开一个社群转战另一个社区无缝衔接……我认为这正是社区问责机制的缺陷，因为我们根本不存在真正的社区。但伤害仍在延续，对此该如何应对？尤其面对那些顽固抵抗者时。”
Carl 50

活动家亚文化尚未形成完整的成熟社群。首先，它缺乏跨代传承的长

期发展。该圈子中很少有年逾四十的活动家，更没有长者提供稳定的支持或指导。在参加一场关于问责制的年轻活动家活动后，我尤其意识到长者缺失及跨代信息传递的断层。我听着他们纠结于问责制相关的问题——而所有那些问题正是我和其他前辈曾亲身经历过的困境。虽然存在小册子，但并没有统一分发，也没有集中存储这些信息的场所。卡尔在访谈中指出，前辈确实存在，但已被隔绝于亚文化圈之外。

"我认为他们确实是资深人士，但我们缺乏将他们视为前辈的文化。很多年轻人追求解放，秉持'别管我'的态度，根本不会听取他人意见。如果有人表现出权威姿态，那就不够'酷'，不符合无政府主义精神。"
1:14:30

去年，当我参加一场在无政府主义空间举办的转化性正义讲座时，在场者皆是年轻且相对新晋的活动人士。提及五到十年前创立特定组织的活动家时，几乎无人知晓那些名字。虽然有人了解转化 x正义相关的杂志和网站资源，但我们收集整理的大量资料并未传承给新一代。

社群内部的亲属关系也较为稀少。除年长者外，儿童数量极少。当活动人士生育子女时，往往得不到他人支持（Rae 2008）。活动家群体的动态很少影响家庭关系，工作也不局限于与其他活动家相关联的领域，日常生活中与社区外人士互动十分便捷。虽然被逐出社区是件严重的事，但其后果未必等同于传统稳定社区中的同类处境。

维系并构成亚文化的是文化共性；但这种亚文化本身就蕴含着流动性。朋克和青年文化常伴随着因工作或求学而迁徙旅行，或是乐队巡演，抑或单纯渴望改变环境。本次研究的所有访谈中，活动人士的迁移与离去都被视为重要议题。李估计该社群中约三分之一成员居所稳定，三分之一停留四至五年，最后三分之一则处于流动状态。社会机构虽可成为社群锚点，但同样会发生变迁：社区空间房东拒绝续租，激进书店与活动场所关闭，集体生活空间解散。

破碎的社群

尽管对社群存在的看法不一，但在访谈和杂志中，许多人谈及激进分子两极分化的过程，以及由此导致的社群分裂或瓦解。在杂志和访谈中，这被描述为一种令人沮丧的经历。"回望这段岁月，我仍被悲伤淹没——曾目睹这个群体凝聚成惊人的抵抗力量，却最终被性侵事件与操控行为撕裂殆尽"（David 108）。在历史性杂志《我们村的锤子》中，作者告诫读者：虽然这不应阻碍幸存者发声，但现实是"当你的团体或圈子遭遇性别暴力事件时，团体很可能分崩离析，人们会受伤，某些人（多为幸存者及其支持者）将被孤立"（21）。这种预判或许悲观，但当暴力事件发生时，预见社群的裂痕实属现实。

具体而言，在我们的访谈中，亚历山德拉谈到了一个问责流程，该流程导致社群分裂，并成为他们离开该社区的原因之一。

这符合标准模板。一对交往已久的男女……分手后，女方向男方指控……一次性侵犯事件。尽管我们这个社区的许多成员参与过无数类似事件的处理，尽管我们撰写过相关文本、举办过研讨会、参加过专题会议……我们拥有如此丰富的集体经验可供借鉴。但这次就像迎面而来的火车，我们无处可躲……有人……看清了看似相当明显的情感虐待模式正反向蔓延。有人洞察到远比男性压迫女性更复杂的权力动态。有人看清了指控及其衍生的效应如何被用来巩固社交圈内的权力……当人们开始争执时，这场冲突便演变成代理战争—因为彼此关系错综复杂，创伤史又如此纠结。人们借着这次问责事件的战场，发泄着积压了十年的矛盾：未解决的性别关系紧张、在经历困境时没有能获期待支持的怨怼、对某个人或另一个人莫名憎恨的执念—无论理由是否正当……而这些政治分歧又映射出更多对立：倾向起义的无政府主义的人高喊 "痛扁那个混蛋！"，而另些人则以特定方式理解女权主义："我们必须相信幸存者的陈述，无论如何。即使这与我们的经历完全不符。" 简直是特么一场噩梦。整个社群彻底崩溃……最终被指控者完全陷入社交孤立，大部分时间只能泡在工作场所或与［新伴侣］相处……直到某天一群人觉得他没按他们的要求行事，直接砸碎了他的车窗，用油漆喷上"滚蛋"之类的字眼。而这一切发生在单亲妈妈家门外……事态变得极其恶劣，所以他……离开了再也没回来……当幸存者得知真相时，简直惊骇万分。整件事就是一场彻头彻尾的灾难。

在亚历山德拉的案例中，情况尤其令人沮丧：尽管社区中许多成员都意识到问责流程可能存在的问题和陷阱，但社区的分裂仍无法避免。那些在多重裂痕中抗争的社区成员所拥有的社交资本和文化资本层层交织，导致无法建立明确的流程或途径来弥合伤害。当幸存者的经历与其政治立场相悖时，从事此类工作的人们对幸存者的自动信任与支持也变得难以维系。

行动主义的转变

问责机制的实践经历促使部分活动家转变其行动主义的形式或类型。在受访者中，那些仍坚信问责制或参与同意权相关工作的人，其行动主义往往受到问责制的塑造，或直接以问责机制为核心。

> "我认为[问责流程]本身就成了我的行动主义...我依然参加示威活动，但投入不再那么深...这需要耗费大量情感能量，而这项工作似乎值得全情投入...就像，这才是我在运动中的角色...从更宏大的意义上说。这让我感到自己做出了贡献。"— James 34:10
>
> "我确实发现这套框架曾主导我一段时间的工作，也认为每个人在特定角色中最具价值...而这次我真正意识到...'哦，这是我能贡献的技能'—不想只是空降现场...我思考的是'我能做些什么有意义的事？'"— Eva 1:29:00

对其他人而言，参与问责流程导致其行动或"社群"发生转变。部分原因或许在于流程参与者的构成，以及在与顺性别男性、有色人种和/或酷儿LGBTQ行动主义亚文化群体共同参与行动后产生的警惕性——这正是被提及的转变之一。在《首张7寸唱片更胜一筹》中，妮娅·金以讲述自身社群转型结束了她的小册子：

> "我不再渴望被那些躲在'激进'生活方式政治背后的人接纳，也不愿与那些不愿翻垃圾桶觅食、无力为表达立场而被捕的人合作来推动真正变革。如今我拥有更美好的归属—一个由酷儿活动

家和有色人种活动家组成的社群，他们的价值观与我更为契合，并接纳真实的我。"

离开社会运动

这种孤立感与支持缺失通常导致年轻女性彻底脱离活动家群体。这种循环已然成为亚文化圈的常态，被视为理所当然的常态。"在许多激进圈子中...尽管男性年龄分布多元，却难见到年轻女性身影。为何？因为年轻女性往往受男友邀请进入圈子，最终沦为性对象，继而厌倦男性主导的圈子而离开"（Said the Pot）。女性身份的活动家们"始终保持沉默...因不堪忍受而悄然退出我们的组织与运动，更因揭露压迫与虐待而遭驱逐"（INCITE! 2005）。

尽管大型行动主义目标遭到破坏，但经验丰富的女性及酷儿活动家们的不满与缺席，通常并未被视为亟待解决的问题。"还有什么比女性和/或酷儿群体因屡遭欺骗、羞辱、身体/言语/情感/性虐待而离开运动更令我们瘫痪的？... "没有什么比厌女症更能阻碍运动建设了"（莫里斯）。尽管有人认为为了维护社群和谐，"当异性恋伴侣分手时，女性离开现场的情况应当是例外而非常态"（Why She 2009）。

社区与变革性正义的话题在活动家群体中始终极具争议性。"如何应对这一问题频繁引发讨论，几乎每次都导致激进社群内部分裂"（Said the Pot）。正如必修课题所示，关于转化性正义和安全空间重要性的观点存在性别分歧。这一现象在关于行动现场安全空间的系列网络帖文中尤为明显。以下摘自劳伦·德尼齐奥（Worriers乐队女权主义主唱、前For the Birds成员）在网络杂志中发表的关于安全空间的初始文章：

> 当我想象一个没有性别歧视的场景时，脑海中浮现的是这样一幅画面：我们有意识地努力为所有人创造更安全的空间，无论他们是谁。所以即便我们不再说"你不能加入乐队或参加演出，因为你是女生"，仍有许多其他行为在我看来充满性别歧视...你知道什么让我感到不安全吗？当你是舞台前区唯一没收到"别用全力撞向体型力量都远逊于你的人"提示的男性时；当你在演出中脱掉衬衫

时。当男性乐队成员说我们四人同属一支乐队后，你却问我"你是乐队成员还是成员的伴侣"。当你说"你吉他弹的真不错，毕竟是个女人"的时候。当你宣称"所有男人都想操那个女乐手"的时候。当你讲强奸笑话的时候。当你使用"婊子"或"荡妇"这类词汇的时候。这样的清单永无止境。（2011年）

该帖引发强烈反弹，涌现大量网络评论、转发及回应。尽管数量庞大难以逐一回应，但许多评论将性别歧视的矛头指向了这位女性亚文化实践者本人。

激进左翼亚文化群体中层出不穷的问责制实践及其引发的反应，导致内部矛盾激化，最终导致某些运动走向终结。尽管时代背景已然改变，但围绕性侵与性虐待的动态演变，与早期新左派运动中的情形惊人相似。塔玛拉·诺珀的陈述——"许多人告诉我，他们'惊讶'于我竟能'忍受那种狗屁玩意儿'，因为与'软弱的女人'不同，我是'坚强'且'政治化'的女人"——这段话如果出自黑豹党或气象人组织的自传，也毫无违和感。亚文化中显然存在亟待解决的问题，但问责机制是否真正触及这些症结，尚不明朗。

[image]

结论

我的研究发现，社会正义领域中的文化实验正试图解决主流文化中普遍存在的不平等问题。行动主义中的预示政治必须应对刑事司法体系相关的问题，以及性别不平等、强奸和性侵等议题。活动家们正在构建替代性结构，试图在主流机构之外创造更具良知与伦理的文化。

尽管致力于满足女性、跨性别者及非二元性别群体的需求，转化性正义的实践与问责机制的落实似乎未能奏效。个别案例或许成功，但整体实践中该模式效果不彰且可能具有破坏性。问责机制虽非蓄意为之，却未能有效解决亚文化内部问题，同时重现了对刑事司法体系的部分批判。

性别相关问题在新左派运动史上由来已久，并延续至当代运动。尽管不同程度地承认了这些问题，但像学生争取民主社会组织（SDS）和黑豹党这样的团体要么未能解决问题，要么最多只是采取前后不一致的做法。在组织建设、领导层构成、分工安排及性关系中边缘化性别议题的行为，最终导致女性自身遭到边缘化。纠正问题的责任始终由性别歧视的受害者承担，而非整个社群共同分担。

性别相关问题由来已久，但近十五年来，活动家们尝试建立DIY体系聚焦性侵问题。当前社会运动中采用的途径应用随意，最终结果也参差不齐。布迪厄提出的社会资本、文化资本及实践等概念，为剖析文化内部权力动态提供了工具。不断演变的预示政治实践正挑战着我们对虐待行为的定义与认知，尤其在活动家所倡导的"社群"语境中。正如众多活动家所言，当私人即政治时，人际关系与实践行为理应遵循伦理准则，植根于激进价值观。

虽然在具体实践和“安全空间”政策上存在分歧是预料之中的，但在激进左翼亚文化内部，关于“性别不平等是否存在”及其重要性的基本认知争论，却出人意料地激烈。对于部分活动家而言，性别平等是左翼行动主义和摆脱国家依赖的基石。这些过程的演变结果，不仅是对预示政治考量，更关乎社会运动的延续性与生命力。

分析与实证发现

亚文化中的预示政治

在既有的不公正社会中构建崭新的社会正义体系和文化实践，本质上存在着一场本体论层面的斗争。参与者皆非来自"革命天堂"，而是深受主流文化中的性别歧视、种族主义、阶级偏见等观念熏陶。要批判性地反思人际互动、潜意识假设及深层结构，往往困难重重。

将基于"社区"存在的框架应用于亚文化时，活动家们面临着固有困境。通过自我认同为社区，活动家们暗示着超越休闲风格选择的整体生活世界。问责制依赖于社区文化的凝聚力 —— 这种文化已确立可被违反且必须处理的规范。此外，问责过程还需社区作为凝聚体对违规行为作出回应并追究责任人。尽管我曾论证其团结并非基于社区，

而是源于一种孤立性，这种孤立性可能在活动家彼此的互动关系中遭到破坏或瓦解。

由于这些政治化动态发生于人际关系中，社会资本与文化资本影响着问责制的每个环节。正如主流文化中那样，亚文化中的权力关系同样决定着：施害者或幸存者能否获得其他活动家的支持；施害者是否被追究责任；双方运用或抵制标签的能力；抵抗行为限制或制裁的能力；以及其行为被视为赎罪的易难程度。

刑事司法的替代方案和矛盾

由警察、法院和监狱构成的刑事司法体系，是备受批判的主流制度之一。尽管人们努力避免简单复制，但幸存者与施害者的二元对立，仍深深植根于刑事司法体系塑造的正义认知中。创建一种既能解决正义、问责和转化的问题，又没有种族主义、阶级主义或偏见的新型替代性社会机构，面临诸多困难。此外，要构建一个既能有效打破善恶二元对立，又不使受害者再次受创的框架，似乎必须对互动行为及其文化背景进行批判性审视 —— 这本身就近乎不可能。

看似矛盾的是，转化性的话语本身并不利于实现转化，反而维持着二元对立的原貌。幸存者永远无法摆脱幸存者的身份，对其行为进行批判性反思的空间极为有限。施害者仍可能被称为"罪犯"，即便其试图完成一个组织混乱的流程或成功完成某个流程，仍可能被贴上这样的标签。尽管问责制以幸存者为中心，但幸存者无权决定自己的成功或终点。

最终，作为转化手段的问责制目的本身也受到质疑。当正义被局限于当事人的“转变”时，活动家们就被剥夺了惩罚和复仇的动机。这种对愤怒、挫败感及暴力行为的否定，尤其值得关注 —— 毕竟该群体向来将这些情绪指向政府与主流文化。有人指出，囚犯能获得的疑罪从无待遇，同为活动家的同伴却无缘享有。另有观点主张：如果幸存者意愿，其支持者应有权对施暴者实施肢体暴力。该亚文化在策略与理念上并非反暴力，却强烈反对报复性暴力。关于活动家群体是否应适用低于或高于普通民众的标准，目前尚无明确界定。

混合性别运动中的女性主义政治

将政治信念应用于性别化人际互动时，往往充满模糊性且具有破坏性。领导层、会议机制、分工体系及安全文化中持续存在的性别割裂，折射出对男性特质的固化崇拜。诸如"男权统治"、"兄弟主义"或"兄弟社会主义"等术语虽揭示了这些问题，却未能提供解决性别（或种族、阶级）动态关系的途径。除非涉及性侵事件，否则个体在人际交往中遭遇性别歧视时只能独自应对。

安全空间的建立与同意机制的完善，旨在为亚文化实践制定切实可行的规范。性实践的文化复杂性已超越简单的同意/不同意二元框架，正转向积极同意的理念。该亚文化秉持性积极态度，常举办深夜派对及各类活动，期间可能涉及药物与酒精。然而，对于性积极理念本身及其对同意可能产生的影响，尚未形成充分的反思意识。人们已意识到虐待定义的扩展及亚文化中虐待类型的特殊性。女性、跨性别者、非二元性别者——尤其是幸存者群体——承担着耗费大量时间精力的行政调解工作，这可能导致额外的压力与职业倦怠。

可能的解决方案

我发现有两种观点认为，解决性别动态关系可能需要通过自主组织，或限制与顺性别男性活动家的个人及性关系。由此，部分女权主义者开始质疑"私事即公事"的表述，呼吁划清个人与政治的界限。这些论点具有双重性：在政治领域，焦点可继续集中于当前的政治项目；而在私人领域，幸存者可私下处理问题，无需寻求更大"社群"的正当性或合法性背书。正如小册子《没有安全的空间》所言："通过反复要求女性必须将诉求'政治化'，最终导致她们用政治话语描述极度私人的事件"（18）。

尽管其中某些论点因其简洁性颇具说服力，但我认为将个人与政治割裂开来并不现实。从政治层面看，我们承认二者相互交织。诸如交叉性、身体自主权、性侵和身体侵犯等问题，在亚文化圈与主流文化中都具有强烈的政治属性。至于限制个人关系，参与社会运动的重要动因正是来自朋友和爱人的情感纽带。必须认识到，社会运动本身往往是充满乐趣的社交体验。即便考量问责机制的缺陷，其最强大的优势仍在于活动家们围绕情感支持建立的社会联结。

为亚文化面临的问题寻求解决方案或疗法实属不易。我的研究揭示了问责制三大困境：

- 1）在形态模糊的亚文化中推行社群化策略的难题；

- 2）构建替代社会机构的灵活机制的复杂性；

- 3）践行性别平等，尤其在不可避免的性关系中。

所有这些挑战都发生在人口流动性强且不稳定的亚文化群体中——他们持续参与主流机构文化实践。

这些问题中的第一个看似自相矛盾。社会运动亚文化既不是社区，又是一个可能瓦解分裂的社群。在宣称社区地位时，亚文化将对新社会的预示性渴望与日常生活中的政治实践混为一谈。尽管可能存在社会依存关系，但活动家们并不依赖彼此谋生、居住或育儿，他们之间也不存在牢固持久的亲属纽带。尽管无法构建传统社区那样的关系网络，但亚文化中若能增加跨代际参与，将有助于形成某种稳定性。具体而言，"长者"可协助实现信息与技能的代际传承。然而正如第一章所述，社会运动本质上是动态进程，其特性决定了它缺乏社区所需的稳定性。

此外，整合非激进的、具有同理心的组织和团体，有助于在存在经验更丰富、资质更高的群体时限制DIY模式的使用。DIY志愿者模式难以持续满足流程所需的情感投入与时间成本。既有社会机构不仅能减轻个体活动家的负担，还能避免不必要的官僚体系与政策层层叠加。如果能借鉴我采访中某位活动家的案例——让更多转型为心理健康及社会工作专业人士的资深活动家持续参与——这两种可能性或许能实现融合。

这三大核心议题中最后一项尤为棘手。单纯要求人们避免性别歧视无法解决问题。由于性别互动根植于更宏大的文化语境，青年群体在性别定义与交叉性理解上的自由派转向，预示着长期变革的可能。鉴于亚文化在某些方面处于变革前沿，预防性的规范构建与旁观者干预机

制的实践探索，展现出积极的前景。

总体而言，这些预设或许能缓解问题，却无法彻底解决问题。作为文化群体，应制定策略应对各类内部冲突，减轻社会资本与文化资本的影响。尽管亚文化批判权力动态，但要对抽象而情感化的社会文化权力实施制衡，尤为困难。

我们缺乏鼓励建设性批判的文化基础。活动家们虽掌握着反思性与特权意识的术语，却难以接受批评。这并非主张回归"民主社会学生会"式的批评与自我批评会议，但承认过错并承诺未来变革的能力，本就不属于我们的文化基因库。主流文化——尤其在政治娱乐领域及#MeToo运动中——已证明否认过错能为个人带来利益。就转化性正义而言，即便变革发生，其价值也常被忽视。要构建更具社会正义性的运动，我们需要一种能容纳建设性批评的政治生态。

研究意义

社会运动内部的人际互动关系，决定着参与者的构成、政治目标设定以及社会运动组织的可持续性。在运动亚文化中，该议题的重要性促使活动家们举办工作坊与培训课程、编写主题刊物、设计教学大纲、投入大量个人时间、组建团体乃至终结社群。尽管活动家们为此投入大量心力，但这些实践的具体实施方式、应对性侵问题的实际成效，以及对行动主义亚文化的影响仍存诸多疑问。虽然部分活动家关注这些议题，但无论是活动家群体还是学术界，都可能因认为这些问题不如活动组织既定目标“重要”而将其边缘化。

活动家是主流文化中的"煤矿金丝雀"，他们关注的问题和建立的文化规范，往往预示着更广泛的主流文化变革。当代关于#MeToo运动的讨论，涵盖了活动家十五年来持续探讨的核心议题：刑事司法体系的正义缺失、性别与性侵议题中微妙的文化权力动态、何时应揭发施暴者或强奸犯以及幸存者遭遇的反噬、性别议题与交叉性议题的平衡重要性，以及不应将幸存者经历局限于顺性别女性体验。"问责"与"变革性正义"正日益成为性侵及人际暴力领域的主流话语。

如果活动家的目标是建立团结，就不能纵容不公，边缘群体也不应继

续被边缘化。如果目标是创建以相互关怀为核心的活动家社群，则需要深入研究退出社会运动者的现象及活动中的性别化劳动。如社群中存在将性别歧视视为政治目标边缘问题的人，那么其他形式的社群正义恐怕难以解决这些问题。

问责制与转变性正义的未来

尽管活动家亚文化圈早在十五年前就开始使用问责制的话语体系，但这个话题至今仍备受关注。2019年春季，巴纳德学院举办的"构建责任社区"活动爆满，候补名单爆满，主办方要求参与者通过直播观看。2018年秋季，激进组织"去殖民化此地"与纽约自由大学联合举办了"责任文化/Culturas de Responsabilidad"主题活动。2019年夏季，布鲁克林无政府主义空间The Base举办了由无政府主义黑十字组织主持的"迈向转变性正义文化"活动。不可否认，这个议题对激进左翼活动家亚文化的各个分支依然至关重要。

当我参加后者活动时，惊讶地发现历经六七年的积累资源竟已从新一代活动家中消失。现场年轻活动家既没有见过我提及的杂志，也缺乏前辈们在实践性政治探索中积累的试错经验。几个在线档案库的消失，意味着大量文字资料如今散落各处，更难寻觅踪迹。

正如第三章所引用的若干新左派活动家自传所指出的，人们确实担忧社会运动无法吸取先前运动的教训。激进左翼社会运动在性侵问题及性别化人际关系动态方面存在严重问题。遗憾的是，尽管问责机制或许能提供建议，但它并非解决这些问题的有效方案。

[image]
[image]

直击性骚扰和性侵犯的根本：超越米兔S09E03

[image] 关键词	女权主义 性侵 权力关系 父权制 等级制度
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月4日
[image] Description	关系结构革命

问题并不在于男性的本质，而在于父权制 —— 这种权力分配的不平等。只要权力支配关系还存在一天，掌权者就必然掠夺弱势群体，无论掌权的是谁。

- Table of Contents

  本土性侵史简述
  企业无法解决问题
  刑事司法体系无法解决此问题
  从交叉性视角审视性骚扰
  是权力，而不是性
  那么我们该怎么做？

[image] [image] 三名自由船队参与者在2025年10月被以色列当局逮捕和拘留后，公开指控以色列部队进行严重的性虐待，包括强奸和酷刑。

过去一年，关于权势人物 —— 几乎清一色是男性 —— 对弱势群体实施性暴力的揭露浪潮席卷而来。#MeToo运动为无数勇敢的幸存者提供了发声平台。

然而，尽管部分施暴者已为其行为付出代价，我们距离解决男性性暴力问题仍相去甚远。

聚焦个别男性的恶行往往只是将其个案化，仿佛他们的行为发生在真空环境中。这种做法与刑事司法体系的运作机制如出一辙 —— 后者着眼于个人罪责；也符合改良主义政治的逻辑 —— 认为只要让合适的人掌权，现行政府和市场经济就能完美运转。

但当如此多男性的恶行浮出水面，我们必须正视一个可能性：这些绝非个案 —— 这些侵犯行为实则现有社会秩序必然催生的系统性产物。

是否存在既能治标又能治本的解决方案？

本文涉及性暴力描述。提前告知。

[image]

几乎所有近期主流报道都将性骚扰和性侵犯视为与资本主义和等级制度"无关"的问题。当撰稿人承认资本主义和等级制度存在一定影响时，他们暗示这些体系的危害性"可通过改良"加以修正。他们敦促我们借助权力来解决权力引发的问题：要施压企业解雇高管，利用媒体羞辱传媒大亨，借助代议制惩罚政客。简言之，我们竟要借助施暴者赖以维系权力的制度框架来"剥夺"其权力。

恰恰相反，如果不能直面性侵泛滥的根源，我们就无法有效遏制这一现象。

[image] 查琳·巴泰勒创作的纹身，灵感源自珍妮·霍尔泽。

本土性侵史简述

性侵与强奸有着深刻的历史根源。早期殖民者认为原住民不配享有与白人欧洲人同等的道德考量。性侵与强奸被系统性地用作殖民工具。哥伦布的船员、贵族米歇尔·德·库尼奥在信中描述了以下场景，字里

行间毫无羞耻与悔意：

> 当我乘船时俘获了一名绝美的加勒比女子，海军上将大人将她赐予我。我将她带入船舱——她依循习俗赤身裸体——我顿时欲火焚身。我欲付诸行动，她却激烈反抗，用指甲抓挠得我后悔莫及。见此情此景（直说结局吧），我便抓起绳索狠狠鞭打她，她发出震耳欲聋的尖叫，令人难以置信。最终我们达成了某种协议 —— 我敢说她简直就像是娼妓学校里培养出来的。

[image]

延伸：https://matters.town/a/oewbxh1m4b33

延伸：https://matters.town/a/4afjqcl5xo1f

延伸：https://matters.town/a/70x77rm9ysfb

奴隶同样经常遭受性侵犯。这是奴隶制度的核心特征之一：除了从事家务劳动外，被奴役的女性还被迫进行性行为和生育，为奴隶主增加更多的奴隶。

自劳动力出现以来，工人就一直遭受性骚扰和性侵犯。这仅仅是雇主与雇员之间权力不平等关系的诸多表现之一。

[image]

延伸：https://edition.cnn.com/2018/11/01/tech/google-employee-walkout-andy-rubin

在这整个过程中，女性从未成为被动的受害者。她们始终以凶猛的姿态、创造性的手段和多样化的策略对抗施暴者。例如19世纪中叶，一位名叫哈丽特·雅各布斯的奴隶曾与她的监禁者展开激烈斗争；在拒绝其性侵后，她藏身于狭窄的爬行空间长达七年以躲避追捕。最终她逃往纽约并通过法律途径获得自由。作为#MeToo运动的早期先驱，她

向《纽约论坛报》撰写信件详述自身遭遇，并于1860年出版《女奴生平见闻录》，成为首批揭露女性奴隶遭受性侵经历的著作之一。

自20世纪初起，女性组建工会为女工权益抗争，其中就包括免受性骚扰与性侵的权利。黑人女性抗争职场骚扰的斗争促成了首批反性别歧视与性骚扰法律的出台。1993年，洛雷娜·鲍比特遭丈夫强奸后割下其阴茎并抛弃田野，陪审团最终宣告其无罪。这些都是正当的抗争形式。

> 他们围着那截流血的残肢转动，仿佛终于消灭了那头觊觎每个人的野兽，此刻它已失去生机，任人摆布。众人露出獠牙，对着残肢吐唾沫。
>
> —— 节选自埃米尔·左拉*1885*年小说《萌芽》，描述了一群饥饿的女工对商贩尸体实施阉割的场景。该商贩曾以食物为诱饵，强迫她们提供性服务。

[image] [image]

企业无法解决问题

在那些败坏的行为终被揭发的男人中，许多人是“惯犯”，这早已不是什么秘密。如今唯一的变化是企业稍加关注了些。企业媒体刊载了女性的控诉；如果施暴行为足够恶劣，某些企业确实解雇了强奸犯。当性侵指控堆积如山、危及品牌形象时，企业解雇惯犯，我们真该感激不尽吗？

这些企业不过是在堵住最终引发新闻的漏油管道。但谁建造并维系着这条管道？正是它们自己。不要为它们解决自己制造的问题而拍手称快。

这其中很多公司早在多年前就已知晓这些指控，却一直都无动于衷。更糟的是，它们放任这些男性在权力阶梯上不断攀升，直至其连环性侵行为引发全国关注。

换言，这些企业通过提供更多的施暴机会，实际上助长了这些男性的恶行 ——让他们得以持续骚扰、侵犯乃至强奸女性。每当一个哈维·韦恩斯坦的罪行被公之于众，就另有另一个哈维·韦恩斯坦在机构赋权的庇护下逍遥法外，继续实施系列性侵。

为什么公司有动力帮助强奸犯在商界取得成功？虽然厌女症是部分原因，但我们必须看到更宏大的图景。企业的成功取决于其创造多少利润，而非是否保护女性免受性侵。在资本主义体系中，是否驱逐施暴者最终沦为简单的经济算术题：他的存在如何影响利润总额？

以比尔·奥莱利为例。自2002年以来，福克斯新闻与奥莱利已支付数千万美元用于和解性骚扰指控。在此期间，奥莱利在福克斯持续走红，直至2017年1月仍签下年薪2500万美元的合约。尽管媒体曝光最终迫使福克斯解雇奥莱利，但该公司早知其施暴行为长达十余年，并斥资数百万美元封口受害女性。当人们了解到2015年奥莱利的节目为福克斯公司带来了逾1.8亿美元的广告收入时，该公司的行为便不难理解了。

这并非特例，而是企业惯常进行的功利主义计算。设想你是奥莱利的尽责主管。刚发现奥莱利长期骚扰女性的恶行，你便向老板们要求解雇他。即便从道德层面认同你的诉求，他们又该如何向股东解释失去奥莱利这只能下大金蛋的鹅呢？资本主义的本质就是将利润置于一切之上，包括道德与安全。

这种体系也让受害者难以反击施暴者。在高度竞争的市场中，一次挫折就可能意味着职业生涯终结、医疗保障丧失、房租无力支付。女性和跨性别者面临的风险更高，有色人种群体尤甚——他们陷入贫困的概率远高于男性。那些好不容易在经济体系中立足的人，自然会犹豫是否值得冒险失去这一切。而反抗虐待或揭发施暴者往往招致恶果，这早已不是秘密。

性骚扰受害者面临两难抉择：是放任虐待持续，还是冒着失去迫切需要的收入的风险？是举报虐待行为，还是面临被驱逐出境的风险？是否可以直接离开工作岗位而不举报虐待行为？如果选择离开，是否意味着会有其他人将接替我成为猎物？

资本主义、国家机器及其他等级制度，为性掠夺者提供了多种伤害反抗者的手段。奥莱利、韦恩斯坦、艾尔斯、法伦特霍尔德（名单在不断延长）等人惯常伤害或终结那些反对他们的人的职业生涯。

对工作安全的担忧也影响着那些被要求目睹甚至协助施暴者的人。韦恩斯坦常利用员工制造受害者的虚假安全感，在实施侵犯前要求员工出席夜间会议的开场环节，随后遣散他们以便与受害者独处。一位前雇员描述了深夜会议中的一幕：韦恩斯坦要求她向某模特宣称他是好男友，当她表示不愿再参加这些"会议"时，他勃然大怒。人们很容易对纵容韦恩斯坦的员工感到义愤填膺，但不可否认的是，正是韦恩斯坦的权力地位使他得以摧毁他人的生活。虽然我们理应期待他人勇敢地为我们挺身而出，即使面对最强大的敌人，但如果想在需要人们牺牲自我才能相互保护的体系中终结性骚扰和性侵犯，终究是不切实际的幻想。

废除资本主义以及所有将财富和权力集中于少数人手中的制度，虽不能彻底杜绝性侵行为，但能够极大削弱富人和权势者对普通民众施加的胁迫性经济权力。如果没有这种结构性的权力失衡，施暴者便无法操纵他人成为共谋者并使其保持沉默。这听起来或许像乌托邦，但如果真想打击性侵，这才是唯一现实的解决方案。任何集中财富与权力的制度，都无法阻止这种权力被用于胁迫或伤害他人。

[image] 不，真没有

刑事司法体系无法解决此问题

法律无法帮助性侵受害者。全国各地的警察曾多次指控报案的幸存者“虚假陈述”，直到施暴者被锁定并定罪，幸存者的清白才得以证实。即便成功说服警方不以虚假报案罪逮捕她们，性侵幸存者仍可能被监禁以迫使其出庭作证。

移民海关执法局将法庭作为针对无证移民的陷阱。无证移民甚至无法让自己踏入法院而不面临逮捕和驱逐的风险。由此完全可以说，国家系统性地纵容了对证件不全者的性侵行为。

即便警方没有把你扔进监狱，职场骚扰申诉中也仅仅有3～6%的可能性进入审判程序。部分案件虽达成和解，但更多因法律对骚扰行为的严苛认定标准（必须达到"严重"或"普遍"的程度）而被驳回。典型案例中，一名建筑工人控告主管多次扬言要对他实施强奸，却因主管行持续了十天，未达到"普遍"标准而遭驳回。

司法体系不仅惩罚那些试图利用它的人，也打击那些试图自卫的人。在新泽西州4号案中，一群黑人女性自卫反击了威胁和袭击她们的街头骚扰者，却遭到起诉，其中四人被判处3.5至11年监禁，关押在莱克斯岛监狱。

认为法律能终结性骚扰和性侵的观念，不过是父权制的迷思。男性始终以“保护女性免受其他男性侵害”为名，换取对她们的支配权——这正是构成父权制根基的保护勒索体系。事实上，法律正是维系压迫性等级制度的核心工具，正是这种制度催生了各种权力失衡与严重不公，包括性侵行为。

[image]

刑事司法体系加剧了企业领域已显现的所有问题。

资本主义经济中企业隐性地将人扣为人质，而刑事司法体系则通过法律与国家的强制装置将人公开扣为人质。

这是权力向少数人倾斜、对多数人彻底剥夺的极致体现，因而成为恐怖权力滥用的温床。

监狱中的囚犯常遭性侵，施暴者往往正是狱警。

当我们诉诸国家暴力权威惩处施暴者时，实则助长了我们声称反对的权力动态。

我们需要探索一种基于人与人之间问责的司法体系，而非诉诸更高的权威。只要权力集中，虐待就无处不在。

[image]

从交叉性视角审视性骚扰

尽管我们主要从性别角度来探讨这个问题，但"男性"和"女性"的身份只是讨论不同程度权力与特权的代名词。我们听到谁的声音以及如何回应这些声音，取决于种族、性取向、经济地位、能力状况和母语等众多其他因素。在挣脱父权桎梏的过程中，我们必须深刻认识自身特权如何使我们免于他人承受的伤害。我们需要倾听那些在父权制与资本主义体系下最易受伤害的人们的故事：黑人女性的故事、跨性别者的故事、无证工人的故事、贫困者的故事。

我们必须留意当权者试图抹黑哪些人的声音。例如，哈维·韦恩斯坦唯一公开否认的性侵指控，恰恰来自唯一指控他骚扰或侵犯的黑人女性露皮塔·尼永奥。

[image]

是权力，而不是性

尽管女性也会实施性侵犯，但统计数据显示女性这样做的可能性远低于男性。这是否意味着女性天生更优秀、更道德或更少暴力？如果真如此，部分原因在于作为非“男性”群体，她们没有被灌输必须践行父权制毒性的阳刚规范 —— 即视女性为物品，或将自我价值建立在性伴侣的数量之上。男性内化的毒性阳刚特质，正是其性侵女性的根源所在。

有人建议解决性骚扰和性侵犯泛滥的办法是让女性取代男性占据所有权力职位。但问题并不在于男性的本质，而在于父权制 —— 这种权力分配的不平等。只要权力支配关系还存在一天，掌权者就必然掠夺弱势群体，无论掌权的是谁。

[image]

父权制并非少数特定男性的恶行，而是滋生所有这类行为的关系框架。

那么我们该怎么做？

如果不试图瓦解制造性掠夺者的权力体系，仅仅谴责这些施暴者，无异于在沉船上舀水。根本问题不在于宣传、法律、政策或教育的缺失，而在于那些自称“保障安全”的体系反而使我们陷入脆弱境地。

我们必须将应对具体性骚扰与暴力的行动，与决心对抗并瓦解滋生这些行为的社会秩序相结合。面对每一起男性暴力事件，我们都应明确：这并非个别现象，而是社会结构性特征所导致的问题。与此同时，我们需要建立变革性正义的实践范式 —— 既能取代刑事司法体系，又能避免复制其任何特征；同时培育新型人际关系模式，使父权制、白人至上主义及其他权威形式不再主宰我们的人生可能性。无论何种性别，每个人都将从中获益。

让我们携手并肩，咬紧牙关。

[image] “我不是你的猎物，我还有牙齿”——kAt Philbin

By Crimethinc

[image]
[image]

为我们自己负责 - 打破反贼圈子中关于攻击和虐待的僵局：超越米兔S09E04

[image] 关键词	
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月5日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

搬弄权力 - 性癖好与虐待的本质区别 ：超越米兔S09E04

[image] 关键词	性关系 性暴力 权力关系 等级制度
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月6日
[image] **Description**	关系结构革命

虐待的本质不在于脱离语境的孤立行为，而在于关系中等级制度的强加，以及受害者在个人与社会生活的日常层面丧失自主权。虐待是一种系统性的存在，而非孤立事件或系列事件。

- Table of Contents

  语境：身体暴力
  情境：角色扮演
  变态性行为
  性癖好中的虐待
  幸存者自主权
  结论

[image]

对于性癖好 —— 尤其是涉及肢体强力的硬核性癖好，如掌掴、鞭打等等 —— 常见批判在于：其与虐待行为“难以区分”，甚至本身即构成虐待。如果缺乏对虐待动态机制的深刻理解，这种观点往往难以被充分反驳。本文旨在以家庭暴力研究者和理论家的视角，阐述我对家庭暴力的理解，以此反驳上述立场，并揭示这种观点如何严重简化了虐待行为的实际运作机制，以及它如何最终伤害到性癖好社群内外幸

存者的身心。

正如参与过各类性癖社群的人士所知，性癖是一个涵盖多种性实践的广义术语，其中许多实践并不包含本文讨论的任何行为。本文使用"性癖"一词时，特指非性癖批评者用来代表整个性癖群体的性实践：主要是**BDSM**游戏及其他涉及身体力量（拍打、击打等）和权力关系游戏（支配与臣服动态、羞辱等）的性实践。

此举并非认为所有性癖好皆可或应归结于此类动态，而是为使本文能够被更广泛的非性癖好群体所理解 —— 正是这些群体最常将性癖好等同于虐待，并因相关言论而陷入认知混乱，成为反性癖好论调的主要推手。

[image]

语境：身体暴力

无论你对性癖好理解的框架或深度如何，只有当你使用错误且简化的框架来理解虐待时，才可能将其等同于虐待。只要对虐待有充分理解 —— 即其本质和运作机制 —— 这种简化就不可能成立。

将二者等同，恰恰暴露了对虐待的肤浅且片面的分析：你执着于用脱离情境的单项行为清单来界定虐待，而非将其视为持续性的胁迫控制动态。这种理解方式注定无法真正认知虐待本质 —— 如果将个别行为孤立看待，视其为普遍性的虐待，却忽视这些行为在关系权力动态中的具体语境，就永远无法真正理解或识别虐待。

“暴力”行为可能出现在虐待关系中，但施暴者（作为支配与控制的手段）和受害者（作为解放与自卫的手段）都可能（且经常）使用暴力。如果脱离具体情境看待暴力行为，便无法看清虐待的动态本质及权力关系的本质。

[image]

识别虐待行为并非简单统计殴打或辱骂的次数：

我们需将其置于权力语境中审视，分析权力归属所在，并探究这些行为如何强化虐待关系或试图打破这种关系。

如果将“虐待”理解为施虐者通过限制、收买并削弱受害者的自主性来维持控制的整体情境 —— 而非脱离权力关系语境的孤立行为 —— 便能迅速揭穿 "性癖好或BDSM本质上具有虐待性" 这一论点的谬误。

要求他人击打我、侮辱我，或在特定且受控的场景中模拟权力关系 —— 这种情境下我始终处于安全状态，可随时撤回同意 —— 与胁迫控制的情境截然不同。后者中我的同意权受到限制，自主权完全屈从于施虐者的意愿。为阐明此点，我认为暂时跳出充满道德评判的性话题领域，探讨其他同样涉及参与者间身体接触的非性活动颇有裨益。让我们来谈谈摇滚现场的"冲撞区"和拳击比赛。

拳击比赛和人群冲撞都是涉及某种身体力量的活动。然而我们通常不会将它们视为本质上的虐待行为，正是因为它们所处的特定情境最终使之成为游戏形式。在安全的摇滚冲撞区、正规的拳击比赛或有边界的BDSM场景中，都存在既定的规范与实践，允许参与者主动选择体验承受/施加身体力量的过程，同时在其他参与者的共同守护下获得最终保障（尽管承认该实践存在某些固有的身体风险）。在各类安全的社交场景中，参与者可随时撤回同意：你可以离开摇滚乐迷圈子继续观赏表演而不受侵犯，可以退出拳击比赛，可以直接说"不"或使用约定好的安全词，整个场景便会终止。

这并非意味着所有社交场合都符合上述情况。如果你被迫参与拳击比赛，且比赛条款令你感到不安全，拒绝遵守可能遭受惩罚——这种情形我们完全可以且应当认定为虐待。但请注意，上述情境中的虐待特征并非源于拳击行为本身 —— 尽管该行为确实涉及身体力量（且常伴随实际伤害）。真正构成虐待的是控制的语境：当事人丧失自主权与设定边界的能力。在安全拳击赛与胁迫性拳击赛中，身体力量所扮演的角色也截然不同。前者中，参与者完全自愿加入，清楚预期结果，感受到他人保护，知晓撤回同意的安全途径，并普遍享受过程。而后者中，被迫参与者会将身体力量感知为侵犯。不仅如此，胁迫情境下的身体力量往往成为强制因素，迫使受害者因恐惧更严重的伤害而屈从于胁迫环境。

如果单纯采信反BDSM阵营的立场 —— 即假设他们对所有形式的身体强力的担忧皆属真实且正当 —— 我们理应质疑：为何他们不对其他同样涉及身体强力的社会实践提出同等批判？诸如摇滚乐迷冲撞区、拳击、摔跤、冰球等活动同样包含身体对抗，且参与者实际受伤的频率远高于BDSM活动。我认为，这种仅针对性游戏中的身体力量而对其他游戏形式视而不见的特殊关注，暴露了关于性偏差(sexual deviance)和自主权的潜在父权制价值观。

[image]

情境：角色扮演

另一个揭示反性癖批评者核心问题的例子是：他们声称参与BDSM游戏“暴露了内心虐待/被虐待的欲望”，却从没将此标准套用在其他形式的角色扮演上。这恰恰说明他们反对性癖的根本原因，在于将其视为个人反感的性变态表现。难道他们同样坚信：渴望在剧本中扮演邪恶掠夺者的演员，内心深处也暗藏亲身实施暴行的欲望？那些参与真人角色扮演（LARP）或在角色扮演类电子游戏中扮演伤害他人、犯下种种暴行的邪恶角色的玩家呢？在这些情境中，人们在封闭的幻想世界里扮演恶行或邪恶角色，难道就不可能存在除现实施暴欲望之外的其他动机？显然存在其他解释。游戏让我们探索理念，演绎假设。我们模拟搏斗、挣扎、杀戮甚至死亡，并不是渴望在现实中实现这些行为——往往恰恰相反。我们游戏是为了成为不同于日常生活的存在。我们渴望建造城市又将其焚毁，在泳池淹死模拟市民只为见证悲恸、失败或纯粹的混乱 —— 这一切都发生在可随时退出或彻底重置的安全封闭环境中。我们游戏，只因乐在其中！

几乎没有反性癖批评者会断言：你扮演邪恶巫师的唯一动机是怀有施行邪恶血魔法的阴暗欲望。也不会有人声称你因每晚玩《侠盗猎车手》就必然产生偷车撞人的内在冲动。更不会有人认为演员渴望在剧本中饰演不悔改的厌女者，就必然怀有同等的憎恨女性之心。但涉及性角色扮演时，参与者却被认为具有独特倾向——渴望在BDSM情境中实施或承受所扮演的行为。

正如其他游戏形式，人们选择在BDSM中扮演特定角色的动机往往错综复杂，远非"暗藏实施或承受该行为的秘密欲望"这般简单明了，尤其当行为超出游戏的安全边界时。许多支配者真心享受在性游戏中扮

演该角色，但若脱离游戏情境/未经被支配者的热忱同意实施相同行为，他们会感到道德上厌恶和反感。同样，许多被支配者从性游戏中获得愉悦，却绝不愿在生活其他领域遭受真实的支配与控制。让参与者感到愉悦的关键在于——这终究是场游戏。

部分性癖倡导者着重强调这样一个现实：性癖社交圈中充斥着幸存者群体，他们将性游戏作为安全的容器，借此探索那些在性侵或虐待情境中失控的行为，并通过游戏将其纳入完全掌控。虽然这种情况确实存在且值得关注，但性创伤绝非人们进行权力动态角色扮演的唯一正当理由——正如创伤也并非人们在非性情境中进行角色扮演的唯一动机。有人享受这种体验，是因为渴望扮演不同于日常生活的角色；有人出于自我探索与尝试；还有许多人根本无需现成理由 —— 纯粹因为乐趣或愉悦，这正是游戏的本质所在！

变态性行为

父权价值观将性行为本质化为对女性必然/独特的“羞辱”，即便女性自愿参与也是如此，并彻底否定边缘性别群体在保持边界的同时表达自主意愿、对自身需求给予同意的能力。在此更广阔的社会语境中，我们必须高度警惕那些将"非主流群体"的性行为妖魔化为天生更危险或更堕落的政治话术。这种论调具有双重危害性——它反向暗示"主流"性行为与亲密关系天生更安全、更注重同意、更少性暴力与虐待，且更少沾染父权制对性与性欲的理想化束缚。

尽管性癖好社群中确实存在施虐者（下文将对此展开探讨），但许多此类社群都建立了健全的社会规范：关于讨论同意与界限的准则、授予与撤销同意的多种方式、事后关怀的实践，以及对性伴侣需求与界限的关注。另一方面，主流社会对"规范性"性行为的普遍认知，其基本实践和仪式中往往包含更多违背同意的行为。支配、控制以及对父权价值观的遵循，构成了所谓"规范性"或"普通"性行为的背景框架 —— 即便没有发生明显肢体暴力时亦是如此。

反对性癖的立场很大程度上也建立在这样一种观念上：施虐者利用BDSM和性癖社群来"掩盖"他们的虐待行为。这种观点再次基于一种信念，即虐待是一种”个人”且显而易见的病态行为，通常会被社会所

排斥 —— 而现实恰恰相反：虐待行为往往是关于爱情与关系的霸权观念被推向极致的必然结果。虐待行为并非栖身于社会边缘，在最离经叛道的群体中寻求庇护；它实则是我们威权父权社会结构的组成部分。亲密关系中的威权逻辑不断蔓延，对性别边缘群体的支配与控制已成为常态。在此背景下，施虐者几乎无需掩饰其虐待行为 —— 除非涉及最极端的形式。而即便如此，他们往往也无需隐藏这些行径，就能持续困住并控制受害者。

性癖好中的虐待

在性癖好群体中，虐待行为确实存在且屡见不鲜，因为父权社会中普遍存在亲密威权主义的价值观。然而，将虐待与性癖好等同的论调并没有对施虐者构成挑战。事实上，这种论调反而强化了他们的行为，因为这正是他们强加给受害者的论调。他们的目的正是要让受害者相信：虐待是性癖的本质属性，唯有接受虐待与侵犯才能获得性愉悦。认同施虐者的观点非但无助于干预虐待行为，反而会进一步孤立幸存者 —— 使他们意识到，一旦揭露遭遇的虐待，这些指控将被用作武器，不仅针对他们个人，更会攻击其所属亚文化群体，甚至反过来将他们遭受的虐待归咎于自身。

幸存者自主权

虐待行为既不能通过居高临下地告诉幸存者你认为对他们“最好的方式”来对抗，也不能通过将虐待责任归咎于他们自身 —— 将你认为必须令其蒙羞并强行"拯救"的变态欲望归咎于他们 ——来对抗。挑战虐待行为需要在所有社会空间中瓦解亲密关系中的威权价值观，削弱施虐者的掌控力，并拓展幸存者的自主权与行动力。这需要在所有社会场域中建立坚实的实践规范：明确同意的表达方式，确保同意能安全自由地给予并随时撤回，同时让任何为私利而漠视同意的人承担高昂的社会代价。

[image]

结论

将性癖好描绘成比常规性行为更能暴露虐待倾向的行为，本质上是一种对虐待的辩护。现实情况是，虐待或性侵犯具有多种形态，可能呈现出各种不同的面貌。有些表现为赤裸裸的暴力，有些则披着"正常"的外衣。执着于要求人们展现性行为的"健康"或"纯洁"表象（这两种概念都深受父权霸权影响），以此证明其非虐待者，并不能保护任何人免受虐待。这只会确保你身边的施虐者成为擅长表演的伪装者，他们继续编织控制与支配的网络，将受害者牢牢困住。

我认为没有必要将性癖好完全排除在分析与批判的范畴之外。然而，为了对性癖好进行肤浅的攻击而对虐待行为进行如此粗暴的简化，不仅伤害了性癖好群体内的幸存者，也伤害了群体外的幸存者。将虐待简化为脱离权力关系、制度背景与人际情境的肢体/言语行为清单，只会模糊虐待的本质。伴侣间的击打行为，或在双方同意协商的性游戏中进行权力扮演，与真实的性侵虐待之间的关系，恰似参加拳击比赛与在街头遭人殴打的区别。

[image]

虐待的本质不在于脱离语境的孤立行为，而在于关系中等级制度的强加，以及受害者在个人与社会生活的日常层面丧失自主权。 虐待是一种系统性存在，而非孤立事件或系列事件。

即便没有真实可操作的权力存在，人们仍可能玩弄权力概念。同样可能（且常见）的是，在表面看似"纯真"的关系中，实际存在着真实可操作的权力。场景终将结束，但虐待与性侵犯永无止境。施虐者和掠食者无需借助性癖好或BDSM来掩饰其行为动机，因为虐待与性侵犯正是父权体制的根基所在。如果我们真正想要挑战虐待行为本身，而不仅仅是压制性偏差和性游戏的表达，就必须将矛头指向那些削弱人们表达性自主权、捍卫自身边界能力的父权制和威权主义权力结构。

By https://theanarchistlibrary.org/library/lee-shevek-playing-with-power.pdf

[image]
[image]

社群集体如何帮助私人亲密关系中出现的问题？：超越米兔S09E05

[image] 关键词	团队 性暴力 情感问题 纠纷 自治
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] 创建时间	2025年1月7日
[image] Description	关系结构革命

清官难断的烂事儿，社群集体能提供什么帮助？

如果我们自己能解决我们彼此间的问题，我们就不需要警察这类国家机器的强制干预，也就不会被他们趁人之危。作为自治主义者这是我们的政治体面。不论如何我们都要学习如何在混乱中帮助彼此，共度难关。

这里是一份操作手册，您可以根据您自己所在的圈子/社群的实际情况，对其进行无限调整；尤其欢迎更多基于自治经验的深入探讨和实践分享。

- Table of Contents
引言
它是什么？
为什么这很重要？
几句说明
何时、如何、以及对谁有用？
a.

b.
c.
d.
e.
f.
这适用于★和▲“从未建立亲密关系”的情况吗？
支持角色分工
组织协调员
物质支持
情感疏导 (Emotional)
主要内容：
恐惧
悲伤
愤怒
抑郁期
案例一：事情并不总是非黑即白
转化式支持
主要内容：
操作步骤
第一步 —— 找个合适的地点
第二步：基本原则
第三步：记录受暴史
第四步 —— 如果尚未休息，请暂停片刻
第五步—— 复盘记录
第六步：制定计划
针对 ▲
针对 ★
团队间的沟通
调解
案例 #2：关于社区角色的思考
作为支持者如何照顾好自己
如何与他人谈论冲突？
故事 #3
如何对付死性不改的混蛋
故事 #4
离开虐待关系的安全防范措施
以下是给 ▲ 的建议
常见的恶劣行为
行为示例
报警

故事 #5
健康的关系应该是什么样？
结语

[image]

本手册源于集体共创。它绝非个人经历的替代品，我们坚信每个人都应该亲手组建小型组织以探讨这个话题并制作自己的刊物。始终期待能读到更多类似作品。

本刊实践过程：5位不同性别成员组成的小组，每周选定一个主题，在约两小时的会议中展开讨论。

1. 定义：虐待的定义是什么？家庭暴力的定义是什么？

1. 定义：是否存在“两厢情愿的暴力”？

1. 性别歧视和恐同心态如何影响异性恋和酷儿关系中的亲密关系暴力？

1. 主流文化如何助长了家庭暴力？种族主义与移民历史在其中扮演了何种角色？

1. 社区应对亲密暴力涉及哪些核心议题？什么是责任追溯？

1. 对亲密关系暴力事件所有相关方的有效支持应具备哪些要素？

我们绝没有试图对任何问题给出终极答案，只是想探讨这些想法，并从大家各自与该主题相关的经历中汲取经验。我们中有人曾从事非营利性社会工作，所有人都在政治圈中经历过冲突（我们正是那种圈子里有人遇到麻烦时会被找上门的人）。多数人在个人生活中曾亲历亲密关系暴力，无论在童年还是成年时期。虽然我们自己都没有被公开指控施暴，但我们都有朋友遭遇过此类指控。

我们中有些人曾参与过其他围绕这个议题进行探讨的团体，但那些团体都解散了，至少部分原因在于这个话题实在太过激烈。我们把讨论问题理论化，因为我们认为在大家准备好之前，避免涉及个人经历至关重要。到小组结束时，每个人都分享了个人经历，并且感到这样做很安全。我们一致认为，给予充分时间深思熟虑，并信任彼此能共同探讨争议性的问题，是推动对话走向新境地的关键。

同时我们强调必须与熟识且信任的人共同参与——许多人曾经历过陌生人参与的大型讨论或演讲，这类对话往往难以深入。由于缺乏深层个人联结与情感投入，参与者既无法深度学习也难以充分分享。因此我们坚持保持小组规模精简。如果有任何人希望探讨该议题，我们都会鼓励他们组建自己的小型信任组。

这个小组的工作过程令人振奋，这种体验在我毕生的政治工作中都极为罕见。既具有实践性又富有理论性、还充满情感的工作，彻底颠覆了我的认知。尽管听起来可能有些肉麻，但这个小组确实非凡——成员们聪慧、专注且勇敢。仅仅通过阅读这本手册无法重现小组协作的独特价值，这项工作的意义正在于通过与伙伴们的交流所建立的社群纽带。

[image]

引言

它是什么？

- 本手册旨在为近期遭遇亲密关系暴力的人士提供支持性建议，涵盖幸存者与施暴者双方。

我们所说的亲密关系暴力，泛指发生在各种亲密关系中的持续性的虐待或暴力行为 —— 包括恋人、朋友、室友、乐队成员、公社成员、亲密团队、超级英雄团队、共同抚养孩子的伙伴等等。其涵盖身体、情感、性、言语或心理暴力等各类虐待形式（后文中列举了若干常见的恶劣行为）。

- 其中包含提供物质和情感支持的建议，以及帮助人们理解自身经历并为行为负责的支持方式。

我们将这个第三阶段的过程简称为"转化性支持"。支持流程的框架看似简单明了，但切勿被表象迷惑—— 实际情况远非如此。为展现其中的复杂性，我们还分享了生活中的一些真实案例。

为什么这很重要？

- 为受害者和施暴者双方撰写小册子或许显得奇怪。我们这样做是因为：我们相信革命的力量、社区的力量，以及人们改变自我的能力。我们相信互助共进 —— 人非圣贤，孰能无过？尤其在所谓“文明”的病态扭曲环境中成长起来的人，谁都可能犯下重大过失。唯有彼此指出问题，才能在下次做得更好，世界才可能真正改变。

- 目前对糟糕行为最常见的两种反应是：视而不见/否认其存在，或是让其中一方离开。我们拒绝视而不见！家庭暴力是女性受伤的首要原因：其危害程度超过抢劫、陌生人强奸和车祸的总和。在每个社区，包括我们所在的社区。是时候摘下"不关我事"和"我无能为力"的遮眼罩了。粉碎压迫、构建健康社区需要我们所有人共同努力。

- 另方面，如果驱逐是应对暴力的唯一手段，就很容易形成妖魔化的氛围 —— 这既无助于施暴者认清自身恶行，也让亲近者（包括受害者，毕竟双方曾亲密无间）更不愿谈论事件的始末。犯错者往往在某些时刻表现出色，甚至在社群中承担重要的工作。如果我们把每个犯错者都驱逐出去，我们自己的圈子很快就会变得异常狭小。并且赶他们去哪里，那里的人们也不会高兴。

- 话虽如此，但这个过程只有在满足两个条件时才有效：a) 对方真心渴望获得支持，b) 他们愿意改变自己和/或现状。鼓励人们主动改变的方法五花八门，从烹煮美味食物到威胁用靴子踢他们，都算。如果对方真的毫无兴趣，那他们就不值得你费心了。这种情况下你只需竭尽所能阻止他们伤害他人。但切勿轻

易放弃劝说——这需要持久的博弈（包括让所有相关者适当冷静），因为一旦成功点燃他们的改变热情，就将是一场革命性的转变（后文有更多说服顽固者的技巧）。

- 此外，建立社区支持模式能实现早期干预。当人们还处于争吵阶段时，帮助他们理清思绪或许就能避免事态升级为肢体冲突。许多暴力行为的根源在于孤立无援。这种文化深陷于鸵鸟心态，正是导致人们互殴的因素之一。我们查阅了全球各地文化中的家庭暴力案例，发现这种现象确实无处不在。但在某些地区，人们彼此间的联系更为紧密 ——当邻里听见争吵声，他们会主动前来查看情况；或是街坊们手持木棍围在屋前，迫使施暴者暂时离开。在这些地方，亲密关系暴力造成的伤害通常较轻，死亡案例更是凤毛麟角。

- 遗憾的是，这个社会应对亲密暴力问题时，可选的良策实在寥寥无几。警察根本靠不住。当我们遭受侵害时，司法不公体系——这个系统性地针对并残暴对待有色人种、激进群体、酷儿群体及移民的机器 —— 绝非多数人首先想到求助的对象。法院素以放任男性施暴者逍遥法外而臭名昭著，同时却严厉惩罚奋起反抗的女性幸存者。况且监禁手段从未真正帮助过任何人（关于警察的更多内容详见后文）。虽然庇护所和团体咨询等服务在一定程度上有所助益，但社会服务机构的选择范围和视野往往相当有限。在那些社会创可贴机构工作的朋友们，最“好”的情况也不过是超负荷工作且受制于法律体系；最糟的情况是社工根本不在乎，甚至认为社区支持是错误的并试图破坏它。所以要小心。如果你考虑将某人转介到某个机构，最好先做点调查。先了解下该组织的声誉，以及它实际能为当事人提供什么帮助。

几句说明

1、在亲密关系暴力中，或任何冲突里，要分清谁是坏人并非总那么容易。有时，就像经典的"家暴丈夫"情景 —— 男人对女人拳打脚踢、破口大骂，而女人因金钱/孩子等原因无法离开 —— 显然有一个人承担了99%甚至100%的责任。但现实往往并非如此黑白分明。可能是一方出口伤人，另一方扔烟灰缸（尽管人们通常擅长扮演社会赋予的角色）。

无论如何，在这个问题上的语言相当匮乏，现存词汇大多带有令人不适的隐含意味。例如称为"施虐者"容易导致妖魔化，描述成"受害者"会削弱主体力量，而"幸存者"一词则相当于把痛苦等同于价值，而"被控者"一词则涉嫌质疑问题的正当性。

鉴于我们尚未创造出专属术语，于是决定采用符号来替代：▲ 代表幸存者/指控者/受伤害者，★ 代表施虐者/被指控者/最恶劣的破坏者。

2、此外，我们将采用中性的表述。在约90%的家庭暴力案件（伴侣/恋人间的持续虐待）中，施暴者为男性。但我们也清楚，家庭暴力发生在四分之一的关系中，无论异性恋、同性恋还是其他关系。酷儿群体不仅需要能谈论自身关系中的暴力问题，更需要承认女性同样可能成为施暴者。

我们都能展现完整的人性光谱，包括那些糟糕的情感。父权制是肆虐的祸患，无疑助长了暴力行为的存在，但绝非虐待的唯一根源。

3、我们喜欢*#$≠%@&！我们用日常口语写下这些文字，使用社区成员都能理解的语言，因为这个问题正是我们社区面临的困境。我们无意拯救世界—— 至少在今天下午四点前不会；但我们欢迎任何人将这本杂志翻译成其他语种，让它能在不同社群发挥作用。

何时、如何、以及对谁有用？

- 本刊主要面向希望支持朋友的人。

当然，对于渴望获得支持的人来说，本刊同样具有参考价值 —— 能帮助您思考可请求的援助形式。尤其是当当事人处于孤立状态的情况下。许多虐待关系中，双方可能都与朋友断绝了联系；或是因初到异乡而缺乏社交网络，这种脆弱性恰恰是陷入虐待关系的诱因之一。

致▲和★：如果你正经历困境却缺乏亲近之人，请不要羞于开口 —— 致电、发邮件或拜访老友或熟人，以寻求帮助。尽量明确表达你需要

对方提供什么。大多数人类（以及许多动物）都乐于行善，只让他们清楚地知道自己将参与些什么。

- 并非所有社区都有大批人专门等待机会提供支持。本手册可能更适合规模较大或更成熟的社区使用。但这并不意味着你不能根据自身情况调整使用。

如果你的社区支持资源有限，不妨考虑寻求其他渠道的帮助，比如家暴援助机构、法院、甚至警察等（关于报警的更多信息请参见后文）。

- 支持机制要发挥最佳效果，关键在于在危机临头之前与伙伴们共同审视这些问题并深入探讨。

学习小组是绝佳的选择（我们自己的小组就很棒），或者你也可以找个知心好友深入探讨。

即便众人准备充分且表现最佳，危机应对依然难如登天。而如果您能召集社区成员展开讨论，这本身就已经赢得了一半的胜利。那还等什么呢？

- 我们（目前）显然不生活在乌托邦，所以，如果事态已失控，你正赶去帮助受害的朋友时读到这段话，那就行动吧。但有一个条件：千万别妄想独自承担！

支援 —— 如同革命 —— 必需是团队协作的运动。

警告！危险！如果你正想要成为某人的唯一支持者，你终将心灰意冷、精疲力竭。即便身着炫酷战袍，你也并非超级英雄。（支持者及支援团队成员的自我关怀技巧详见后文）

- 有时 ▲ 方会主动寻求支持，但并非总是如此。

如果你发现某人身上有淤青，或者朋友向你倾诉其恋人做过的极不妥当的事，请在行动前先思考如何与对方沟通、以及你打算采取什么行动。

a.

他们可能并没有意识到这种不体面的行为属于虐待。如果想就此与他们沟通，请明确表达此类行为不可接受，但切勿对当事人或★进行道德评判。使用"混蛋""王八蛋""废物"等贬义词指代★，或提及"家庭暴力""受虐妇女"等词汇，可能导致▲产生疏离感或防御心理。

尽管你认为存在虐待行为，但▲很可能依然深爱着★。请具体指出令你担忧的行为细节。

只是说"真糟糕"或"太过分了"，可能导致对方误以为你认为★的行为虽不妥当，但仍在正常范围内。

b.

他们可能不愿面对此事。你可以尝试劝说，但最终决定权在他们手中（★无此选项）。

如果强迫▲接受他们不想要的帮助，那就不是在协助他们解决问题，反而会让你变成又一个发号施令的人。尤其不要在对方尚未准备好时，坚持要求其离开暴力关系。他们拒绝离开可能有充分理由。

在虐待关系中，离开往往是最危险的时刻（79%的夫妻间肢体暴力发生在▲离开之后。详见后文关于离开时的安全注意事项）。

c.

你可能不想处理这件事。你没有义务（或能力）为银河系中每个遇到

问题的人提供支持。

如果他们需要帮助，你可以随时将他们转介给其他值得信赖的人、相关机构或热线服务。

d.

他们或许愿意和解，却不愿谈论发生过的事。

常识告诉我们，沟通能化解矛盾，大多数情况下也确实如此。但研究创伤后应激障碍（PTSD——由创伤引发的慢性心理疾病，包括亲密关系暴力）的专家指出，当人们刚刚经历过极端事件时，立即要求他们描述细节并不是最佳选择。

[image]

最关键的是采取一切必要措施让他们尽快平静下来，给予抚慰并建立安全感。待他们准备好时自然会开口 —— 这个过程可能需要相当长时间，甚至长达一个月。在此期间，你可以通过非语言交流的方式给予支持。

e.

在承诺之前，先想清楚自己愿意付出多少。

人们正经历着各种糟心事，可能感到不堪重负、困惑迷茫，需要各种不同的支持。你完全有权决定自己能承担多少。

与其突然因不堪重负而抽身，不如循序渐进地开始。

f.

审视权力动态。

[image]

性别差异显然并非导致关系中权力失衡的唯一因素。种族、文化、阶级（等等）同样会影响权力分配，更会牵涉安全保障、沟通模式、以及服务获取的渠道。

本手册采用泛指方式探讨权力动态，但建议您在使用本手册时结合具体案例进行思考。

这适用于★和▲“从未建立亲密关系”的情况吗？

本手册针对的是那些彼此的生活已经深度交织在一起的人们遭遇危机的情境，因此其中许多内容也许不一定适用于关系疏远的情况。

情感联结本身就会催生复杂的情绪 —— 愧疚、愤怒、爱意、渴望、挫败、温柔、困惑，抑或彻底的混乱。这种联结可能让人容忍来自熟人的恶劣对待，而面对陌生人时则未必如此。

当事人（★）可能无法辨识对方的恶意，或以陌生人施暴事件中罕见的宽容态度为其开脱。这种动态关系往往持续存在，尽管当事人可能只关注单一事件。

支持亲密关系暴力受害者（转化式支持）的工作之一，就是引导▲和★双方共同审视这种动态关系及各自扮演的角色，承担自身责任，避免重蹈覆辙。

如果▲与★素不相识，上述分析则不适用。但即便如此，协调者的介入以及提供物质与情感支持的建议，仍具参考价值。

[image]

支持角色分工

我们将支持工作分为四大类：生活保障、情感疏导、“转化成长”以及组织协调。

这并不意味着每种支持都要专门找一个人来负责；各项职能之间完全可以、也必然会存在重叠。

而在某些类别中，你可能需要好几个人手（记住，千万别一个人扛下所有！）。▲ 和 ★ 应该拥有各自独立的支持团队。虽然两者的支持形式会有所不同，但这四种角色对双方都适用（只要他们愿意在一定程度上正视并处理自己的烂摊子）。

组织协调员

根据情况的不同，待办事项可能会非常繁杂。因此，找一位协调员来确保信息通畅、并确认受支持者的需求得到满足，是很有必要的。

对于那些提供近距离的、私密支持的同伴来说，他们很容易陷入细节而忽略大局；协调员则负责全局把控，监督原始支持计划是否得到执行。

当其他成员出现倦怠迹象时，协调员要负责寻找替补人员，协助主持或寻找协调人，并提供心理咨询或其他外部资源的联系方式。协调员还可以组织 ▲ 和 ★ 各自的支持团队内部或团队间的会议，共同出谋划策、互通有无，同时防止团队出现内讧。

物质支持

包含：适用于▲或★情况 ——

- 住宿场所

- 食物
- 生活开销
- 托儿服务
- 医疗救助
- 陪同服务 - 往返工作地点、住所或其他常去场所；居家、会议、活动等场合

针对 ▲ ——

- 紧急情况待命人员
- 与邻居/社区成员/室友沟通告知
- ★ 存在安全隐患和/或暂时被禁止接触

在家庭暴力中，当我们考虑▲离开施暴环境时，通常会想象他们搬离住所、投靠朋友甚至迁居他城。这其实本质上是通过令当事人流离失所、东躲西藏、甚至搞砸自己的生活来换取“安全感”。

某些时候这确有必要，但是，安全也能通过为★另觅居所、配备"保镖"等方式来实现。

陪护工作量巨大且并非总有必要，但对▲而言可能至关重要 —— 能让他们获得安全感与支持。如果▲寻求陪同（无论是为了防备谁），即使旁人觉得无关紧要，也应予以配合。▲ 自己最了解自身处境，如果其担忧生命安全，往往确有充分理由（42%的女性谋杀案受害者死于亲密伴侣之手）。

有时，▲ 可能只是不想见到 ★ 出现在面前。根据 ★ 被禁入的空间公共化程度，这可能成了最难协商的事情之一（尤其是当 ▲ 还没准备好公开谈论所发生的事情的情况下），因为这会导致“七大姑八大姨”都来掺和并指手画脚。

不过，将 ★ 从住所、组织、书店或排练室驱逐出去并不一定是永久性的。通常在事态平息后，双方是可以重新共处一室的（尽管这需要时间）。提议先驱逐一两个月，然后再重新评估，可以避免让这个决定显得像生死抉择，从而减少大家的焦虑和防卫心理。

情感疏导 (Emotional)

主要内容：

- 倾听他们的宣泄。
- 向他们保证你会提供帮助。
- 陪他们细化支持/安全计划。
- 鼓励他们勇敢表达诉求。
- 帮助他们以安全的方式发泄情绪。

情感支持角色最适合由好友承担，或者至少是受支持者不反感的人。

情感支持者（ESP）可以挑战受支持者令其去直面自己的问题，但其核心任务是帮助 ★ 或 ▲ 建立足够的安全感，去完成该做的事，并持续参与心理治疗、调解、转化式支持、或“如何避免成为暴力混蛋”之类的课程。

[image]

这不容易：你既要对他们友善，又不能为他们的不健康行为找借口，

同时也不能把另一方妖魔化。

当你担任 ▲ 的情感支持者时，请记住，他们此时的情绪可能极其复杂。这段关系中很可能存在过美好的一面，才让他们维持至今，所以他们很可能会想念对方 —— 哪怕他们嘴上一直在抱怨对方这半年来有多垃圾。他们可能会感到迷茫，只想躲起来。

你的工作之一是列出各种选项，帮他们理清需求，因为他们此时可能无法清晰地表达。但请记住，如果他们需要支持，必须由他们自己决定支持的形式。不要替他们做决定、更不要强加意愿。受害者找回力量的过程，就包括重新掌控自己的生活。

作为情感支持者，你可以帮助人们打开他们的情感之盒，同时不要被倾泻而出的情绪所压垮。当他们进行情感锻炼时，你可以陪伴左右，告诉他们此刻情绪失控是正常的，并协助辨识那些试图悄然涌现的情绪。这些情绪未必显而易见——女性常以悲伤掩盖愤怒，男性则用愤怒包裹恐惧和悲伤。如果对方愿意尝试，可通过不同活动来探索情绪的显性表现。

恐惧

- 不要独处
- 抱着毛绒玩具或宠物
- 开着夜灯，或者和好朋友一起睡
- 不断复习支持方案
- 询问他们还需要什么/想要什么才能感到安全

- 让支持团队与当事人见面，只为传达"我们随时支持你"
- 参加自卫课程/防身术训练 [image]街头搏击基本技巧（转帖）
- 写下感受 你在人际关系处理方面遇到过哪些尬事？贴张便签，我们聊聊

悲伤

- 能哭出来是好事，别怕哭
- 承认经历了挫败 —— 即使是结束一段糟透的关系也算挫败/失去
- 如果相信仪式，可安排告别仪式让当事人向对方/那段关系道别，或者写一封不会寄出的信
- 绘画、涂鸦、写诗 ……

愤怒

- 打枕头或沙袋
- 跑步、蹦迪，或进行其他剧烈运动（注意安全）
- 摔玻璃瓶（注意别扎到小动物）
- 跟着最爱的重金属乐队嘶吼/合唱

抑郁期

- 如果出现嗜睡，要叫醒TA，陪TA出去散步
- 去寻找被丢弃的宝贝/进森林/参加派对/去吃顿好的
- 允许静坐，但别拖太久
- 突然跳起来砸碎某样东西（注意安全）
- 一起读诗

作为情感支持者（ESP），请务必意识到受助者正处于脆弱期。身体接触会变得非常复杂。即使是拥抱、揉背、牵手或依偎这种看似无害的行为，也可能触发痛苦的回忆。他们可能渴望安慰，同时又对被触碰感到惊恐。所以，触碰前务必征得同意。

此外，在深入参与情感支持的过程中，你们可能会产生某种情愫，导致双方关系变得令彼此感到不适（迟早会如此）。一旦发生这种情况，支持工作就几乎无法开展了。所以请务必谨慎，三思后行。

[image]

案例一：事情并不总是非黑即白

我参与这个事，是因为受邀参加一个关于熟人亲密关系暴力的干预会议。起初，情况看起来非常明确：这对情侣在一起几个月了，与朋友们日益疏离，并陷入了频繁争吵又和好的循环。在一次争吵中，男方动手了。在干预会上，女方讲述了他如何先推搡她，然后扇了她耳光。男方垂头丧气地道了歉，承认了一切。我记得当时在想，这种悔恨表现是施暴者的典型套路，希望其他成员不要因为他表现得懊悔就轻饶他。

大家确实没有轻饶。女方表示感谢支持。男方哭了，说他觉得自己应

该分手，去接受心理咨询，并暂时离开这个社群。一切都在按照我预想的剧本发展。

但随后，风向变了。

她开始说想留在他身边，帮他解决问题。他则表示不确定，不想再伤害她，但也不再信任自己在这段关系中的表现。当有人建议他们分开时，她变得非常愤怒，甚至说也许她不再需要社群的支持了。有人提出至少大家应该定期沟通，聊聊他们之间日益剧烈的冲突到底是怎么回事。她坚称这是私事。他保持沉默，最后说："如果你能遵守承诺戒酒，我就留下。" 她反驳说自己没有酗酒问题。

随着对话深入，真相浮出水面：女方长期酗酒、言语虐待，且有砸东西的倾向。而男方试图照顾她、自诩"救世主"以及在她醉酒时强行干预，才导致了那次肢体冲突。男方从小照顾酗酒父母的成长背景也随之曝光。会议结束时，大家终于明白：虽然打人绝无借口，但情况远比初看起来要复杂得多。

转化式支持

主要内容：

- 不带评判地倾听。
- 通过记录受暴史，帮助他们跳出片面局限，客观地审视处境。
- 分析亲密暴力的模式。
- 挑战他们的认知，让他们看清双方在冲突中各自扮演的角色。
- 帮助他们规划未来生活，并制定实现目标的具体步骤。

预警： 开展转化式支持需要类似于心理咨询、心理健康工作、甚至包括街头生存所需的技能。如果你和同伴感兴趣，请先参加专业培训（如自杀干预热线或家暴避难所的志愿者培训），然后先进行角色扮演练习。严禁把正处于崩溃边缘的人当成练习的小白鼠。

此外，最好采取“老带新”模式（例如让“理论派”搭档“实战派”）。你也可以寻求友好的心理医生合作，但要意识到，主流机构往往并不熟悉或不认可这种非传统的转化过程。

[image]

转化式支持 有别于 传统“治疗”，其核心在于 聚焦当下与未来 ， 而非 沉溺于过往。

与绝大多数工作一样，转化式支持也是一项团队运动。由于你不能对组外人员透露任何细节，你需要一个可以一起“复盘”排解的搭档。听别人讲述暴力的细节是很压抑的，你需要一个泄压阀。强行压抑自己是没有用的，被压下去的情绪早晚会在某个咨询工作中以极不恰当的方式爆发出来。

此外，从事类似思想工作的人极易陷入疯狂爱恋，最终与★或▲发生关系。千万不要。当人们处于极度脆弱状态，正努力化解重大情感危机时，发生关系不仅会搅乱一切，更会摧毁你作为支持者的公信力。这无异于助长导致当事人陷入困境的原有动态。所以，如果你开始产生冲动，请尽快与另一位支持者沟通，给自己喘息的空间。

理想的“支持团队”应由两名相对中立的人组成。如果你过度认同受支持者，无法客观审视其行为，请不要参与。对于加害者（★），你需要帮他们打破否认的防御墙；对于受害者（▲），你需要引导他们为自己的生活负责，而非责怪他们遭遇了暴力。

与此同时，▲或★类对象必须足够信任你，才能敞开心扉倾诉，并确信你不会将他们的私人故事刊登在下一期《摇滚至上》杂志上。

但如果你过于中立，完全无法产生共鸣，那你可能只是个局外人，根本无法真正理解这个过程或这个群体。那些最优秀的转化式支持工作

者都曾与内心恶魔搏斗并最终战胜。他们亲身经历过蜕变（未必是亲密关系暴力，也可能是成瘾或重度抑郁等），因此深谙危机各阶段人们可能展现的状态。

危机具有周期性，就像生活中大多数事物一样，无论是对于▲来说还是★，其发展阶段都大同小异。尝试辨别他们所处的阶段很有必要，同时要提醒他们在这个过程中会经历重大起伏。

危机爆发时，人们会进入求生模式，但这种状态无法持久，因为肾上腺素终将耗尽。随后便是震惊期。事态虽已平息，当事人却可能陷入失控、抑郁或触底的状态。

当开始处理问题时，▲往往会感到安全感增强，★则可能陷入自责。持续处理问题会进入危险的蜜月期 —— 他们双方可能误以为已解决所有矛盾。治疗取得进展，彼此道歉，思念之情涌动，于是欢呼着重归于好（或与另一位同样迷人的对象开启新恋情）。最终 —— 或许很快 —— 灾难再度降临。此刻除了事件本身的冲击，他们还会感受到背叛，无论是来自自己还是对方。这将引发愤怒、恐惧、抑郁和挫败感的新低谷，成为危险时期。关键在于认识到起伏本是必然，并以不抱不切实际期望的态度穿越这些波折。

转化式支持（**TS**）应在情绪平复（肾上腺素水平降低）、且对方重新具备反思能力时启动。回溯关系中最糟糕的时刻本身就是极具冲击力的过程，如果时机过早反而可能造成二次创伤（创伤后应激障碍研究者指出，理想情况下应等待2-5周再详细描述创伤事件）。因此请等待危机平息，待支持团队其他成员为当事人提供基本安全保障，且当事人真正做好了谈话准备时再行动。

届时请做好心理准备，因为这将是个漫长的过程。危机本身通常不会超过1-2周，但每个人实现真正转变所需经历的成长历程往往需要数年。作为支持者，你正是连接两者的桥梁。你必须承诺至少与★或▲共事3-6个月（此后你或许可以退出，但他们尚未完成）。你的职责是在初期阶段持续提供支持，直至为他们对接优质的长期援助（参见步骤6中改变人生的活动范例）。

[image]

操作步骤

第一步 —— 找个合适的地点

（此步骤适用于▲和★两种情况）

首要任务是营造安全、舒适且私密的空间。明确告知对方，接下来的讨论是 100% 保密的，且你已经关闭了心中的“审判开关”。

这个过程旨在协助疗愈/康复，而实现康复的最佳方式就是抛开羞耻与尴尬，真诚面对发生的一切。

第二步：基本原则

- 针对 ▲： 明确你只是倾听者和方案的协助者，你没有“魔法药水”，也不提供说教。不要代他们做决定，要赋予他们力量。挑战他们去看清自己在关系动态中的角色，这不代表暴力是他们的错，而是为了让他们学会设定界限、识别烂人。警惕“受害者情结”，不要让他们沉溺于“因为我受过伤，所以我绝对正义”的逻辑中。

- 针对 ★： 必须深入挖掘。提醒他们，如果不能诚实面对自己就注定会重蹈覆辙。你可以分享自己曾经搞砸事情的经历来建立信任。如果“自我成长”故事不足以触动他们，你可以提醒他们：他们的行为影响了社群，如果他们不改变，社群也会按自己的方式做出反击。

第三步：记录受暴史

（此步骤适用于▲和★两种情况；当然，要区分对待）

你可以边听边记录他们的经历，但所有内容都归他们保管。从他们记忆中最先发生的糟糕事件开始记录，无论是言语、身体、情感、还是其他形式的虐待。如果他们从身体虐待开始叙述，请追问是否在此之前就察觉到异常征兆 —— 如争吵、贬低性言论、情感勒索等等，并将这些细节一并记录。持续追溯至最近发生的事件。此阶段你主要负责倾听并引导提问。

从记忆中最早的冲突开始记录。包括：

- 暴力的循环或升级模式。
- 他们曾尝试改变或阻止暴力的努力。
- 生活在虐待中的感受。
- 对另一方的评价（正面和负面都包括）。

对于 ★ 来说，还需要记录：

- 暴力行为的触发点是什么？
- 你在关系中贡献了哪些积极影响？

对于▲ 开始，还包括：

- 他们从中获得了什么？

第四步 —— 如果尚未休息，请暂停片刻

透透气，活动下腿脚，客观回溯下。

第五步—— 复盘记录

（此步骤适用于▲和★两种情况，但不可同时使用）

将记录下的全部内容复述给他们听，补充遗漏的细节。现在你可以发表评论。

回顾暴力循环理论，指出他们在叙述中体现的循环模式。提醒他们暴力是普遍的社会灾难，这些关系模式并非他们独有。

协助他们审视双方各自扮演的角色及自身责任所在。指出你观察到的其优势所在，以及他们在处境中为改变或脱离困境所做的努力。探讨那些阻碍他们抽身离开、助长其为糟糕处境开脱的信念与恐惧。

[image]

为他们寻求帮助的行为给予肯定。

他们的感受、渴望和需求至关重要！

第六步：制定计划

针对▲（受害者）和★（施害者），要分别制定计划（且两人必须处于隔离状态）。

和他们聊聊接下来的选择。尽量引导他们关注自身 —— 改变对方不是他们的职责。他们的目标和渴望是什么？无论是近期的还是长远的，他们希望生活是什么样子的？需要做什么才能实现？

计划的内容可以大到戒毒，小到写日记。任何能强化“新生活”的事物都是好的 —— 远足、武术、吹大号、集体生活、纯素饮食，或者发起一个新的社区守望小组。如果他们正处于抑郁中，难以想象更好的生活，就给他们提供一些积极沟通和关系模式的例子。如果合适，也

可以推荐他们去参加心理咨询、防身术、愤怒管理课程、调解服务或互助小组等。

把计划写下来。开头要简短精炼，不要堆砌太多内容。

计划的成功对★或▲的持续推进至关重要，因此简洁小巧的方案比庞杂繁琐的更有效。计划需包含时间表，并安排支持人员定期跟进。建议频繁修订计划 —— 甚至每次见面时都可调整 —— 通过持续优化确保其实用性与可操作性。

针对 ▲

尽量让 ▲ 自己提出计划的想法。如果他们卡住了，可以提供一些选项，但不要强加于人。接着进行现实评估，分析每个选项的优缺点。

针对 ★

★能够为自己的计划构思方案，▲和社区成员同样可以提出想法。

▲很可能会对★提出具体要求或限制条件。如果此事广为人知，社区成员可能会决定：★如果想参加比如钩织黑色连帽衫的课程，就必须尊重▲的意见。必须建立机制确保★切实履行计划。

★可能真心渴望改变而坦然接受监督，也可能是在磨洋工，甚至是为了得到计划结束后的"胡萝卜"而撒弥天大谎。无论如何，★都需要有人进行监督，确保一切按计划推进。

[image]

团队间的沟通

显然▲和★各自拥有独立的转化性支持团队。但★与▲的团队在整个支

持过程中保持沟通至关重要。★的团队需要明确的施力方向，并协助★制定切实可行的计划。如果★希望加入比如激进啦啦队来释放过剩的攻击性能量，★的团队必须确认▲是否已加入该团体，以及是否曾明确要求★不要参与。

双方支持团队的信息共享还能发现矛盾之处，促使★和▲保持更坦诚的态度 —— 尤其当他们选择共同面对时。毕竟大多数人都会对你撒些谎。别当真。这并非出于恶意，而是背负千斤重担的人难免会不时不时地甩出点什么来。

如果双方都知道自己一方的团队也在获取事实的另一面，就能防止他们的叙述变成“伟大的虚构文学”。这也能帮团队识别求救信号。★ 可能无法开口请求更多的限制或陪同。但如果大家都知道 ★ 被禁止去某地三个月，而他突然随口说计划周五去那里看演出，他可能是在通过这种方式请求别人阻止他。

注意： 团队间的沟通可能很棘手。要警惕双方团队产生冲突，更要防范被 ★ 和 ▲ 挑拨双方关系。也要警惕两边团队联合起来“暗箱操作”控制局面。无论你觉得他们的过程有多不健康，都必须以他们的议程为中心，要尊重他们的自主决策权。

调解

调解可以是计划的一部分，用来解决具体问题，比如同居期间的财务归属、或者宠物的探视权等等。

注意，很多调解机构对涉及家暴的冲突避之唯恐不及，理由很充分：让 ▲ 和 ★ 待在同一个房间里可能在生理或心理上都不安全。有很多不涉及调解的方法可以解决这些问题，所以如果一方不是真心想参与，就绝不要强迫。

调解也可以是防止矛盾彻底爆发的好办法。无论哪种情况，调解都是一个复杂的过程。负责调解的人必须在调解技巧和家暴处理方面都有丰富的经验，否则只会适得其反。

案例 #2：关于社区角色的思考

达伦搬进了我们的集体宿舍。他曾是我们的熟人，但不算深交。他搬进来不久，关于他的前任维尔玛之间的事情就爆发了。知情者开始在社交场合冷落达伦。

随着事情公开，达伦告诉我们，他在萨克拉门托时和维尔玛大吵了一架。他叫她离开，她不走，于是他愤怒地砸墙导致手部骨折，还摔坏了一辆自行车。随后她离开了，关系结束。维尔玛有精神健康病史，达伦曾是她重要的支持者。达伦对自己当时的行为感到非常沮丧和悔恨。他同意参加愤怒管理课程和咨询，并定期向我们汇报近况。

维尔玛要求与达伦断绝一切接触。她写了一本小册子，指控达伦是“性别歧视的暴力虐待者”，并要求把他逐出社区。维尔玛和她的支持团队对我们继续接纳达伦感到非常愤怒，但他们没有直接联系我们。我们听到的指责是经过五手传播后的，说我们“在性别歧视的避难所里包庇暴力虐待者”。

我们组织了一次面谈。我们表达了对维尔玛的支持，但也解释道，我们认为社区在这种情况中应扮演不同的角色。我们觉得需要接触达伦，给他支持去治愈并改变他的愤怒反应模式。维尔玛却认为我们不支持她，加剧了她的精神问题。

我担心的是，人们躲在背后议论纷纷却不做任何改善现状的事，还自诩在“反抗性别歧视”。在我看来，这种行为只会让当事人的处境变得更加艰难。

作为支持者如何照顾好自己

首先，当你成为支持者时，你承担着巨大的责任，这需要大量的时间和精力。因此，如果你开始感到压力过大，请务必抽出时间照顾好自己。

请记住：你并非完美无缺，也无需承担拯救生命或阻止他人受创的责任。你的存在是为了提醒对方健康尊重的关系应有的模样（参见第38页建议），并鼓励他们重拾自我认知和人生愿景。失误在所难免——尤其当被支持者自身需求模糊不清时——请勿苛责自己。

暴力事件对所有相关者都是创伤，包括支持者。当你承担这项工作时，务必为自己预留空间来应对即将听到的糟心事。最好在远离受助者时处理这些情绪 ——他们通常心事重重无暇分心（尽管偶尔也会感激那些愿意与他们感同身受的人）。

为了不让自己感到精疲力竭，一个好办法是持续与其他支持者沟通。这可能意味着开个会（或者更好是办个晚宴），让所有支持者聚在一起聊聊。当你感到不堪重负或无法胜任某事时，能够给这些支持者打电话非常重要。这也意味着要清楚自己的极限，并让别人知道你的底线在哪里。

最难处理的情况往往是事后的余波。如果那对情侣决定复合，支持者可能会觉得这简直操蛋，感到心力交瘁且愤怒不已。作为支持者，你听到的多是负面传闻和挫折经历，这会让你觉得分手才是唯一理智的出路。但感情很少全是烂事儿，当一个人寻求支持时，这段关系中美好的一面往往会被略过。所以，为了不让自己发疯或对朋友彻底失望，你必须记住：过程比结果更重要。

如果你开始觉得“绝对应该这样做”，那么你支持的对象可能会因为你的压力而失去自主选择的能力。这会将人困在“受害者模式”中，导致无力感。这对支持者来说也是一种压力，因为你必须承担为他人做决定的重担。最终，这会让你疲惫不堪，而对方也没有真正学会自己做决定 —— 这一点对他们未来进入更健康的恋爱关系至关重要，否则只会不断重复以前的破事儿。

另一种经常出现并可能导致更多创伤和闹剧的情况，是你与被支持者之间发生了性亲密。当人们脱离糟糕的处境时，往往在寻求安全感和与他人的联结。这会让他们变得极其脆弱，并可能转向你寻求这种联结。性亲密是建立联结的一种方式，但如果你发现自己产生了这种感觉，请退后一步，等到对方脱离那段关系足够长的时间、能够清醒地思考他们到底想和你建立什么样的关系时再说。

[image]

如何与他人谈论冲突？

作为身处其中的支持者，可能会有很多人问你发生了什么。你回答的方式在一定程度上决定了流言的走向。保持诚实且不危言耸听非常重要。如果你正对其中某个人感到生气，这可能很难做到，但请记住：试图抓住“坏人”进行私刑式的围攻，极少能改善局面。

同样重要的是，要询问被支持者希望透露多少细节。他们可能不希望所有人都窥探自己的隐私；或者他们根本不知道自己想要什么。如果是这种情况，给他们一些选项，比如：告诉大家 x、y、z 的事可以吗？我是不是不该说任何细节，只说你们最近很难熬？有没有哪些人是你特别想让（或不想让）他们知道情况的？

提问时要尽可能具体、清晰。确保花时间鼓励你支持的人向你明确表达他们的需求。在不引导他们走某个特定方向的情况下做到这一点往往极其困难，但只要有时间和耐心，被支持者及其支持小组总能找到行之有效的方案。这可能很难达到平衡，因为支持者对自己分享信息和保守秘密有自己的想法，这些想法必须得到尊重 —— 即便不一定要完全迎合。

有时流言会失控，社区里的每个人都在乱嚼舌根。这种时候，把双方的支持小组聚在一起谈谈真相是很有帮助的。确保有一位优秀的调解人。在这种聚会中，可以鼓励参与者建立联结，记住大家同属于一个社区，都希望有最好的结果。然后，大家可以共同决定不再参与散布流言，并让其他乱说话的人“闭嘴”。

故事 #3

我有一个朋友叫小米。她的老朋友小凡和女朋友艾玛被房东赶了出来，需要找个地方落脚，直到找到新住处、决定是否离开该地区，或者决定是否去戒毒（他们吸食冰毒成瘾严重）。尽管许多朋友感到担忧、挫败和愤怒，小凡还是动过手打女朋友。尽管艾玛的许多朋友也感到担忧、挫败和愤怒，她还是不想离开小凡。

小米不允许小凡在住她家期间打艾玛，并和他们谈论过两人的关系，但感觉没什么回应。

很多人不同意小米的做法，认为小米给这对情侣提供住房是在支持他们的“不健康关系”。小米则认为，让他们有地方住总比流落街头好，而且大家住在一起时小凡打艾玛的次数确实减少了。

这对情侣最终搬到了郊区。他们还在吸毒，但没以前那么频繁了，而且似乎没再发生暴力事件，尽管这很难说得准。

如何对付死性不改的混蛋

并不是每个人都会张开双臂拥抱这个解决过程。通常情况下人们很难面对自己的破事，他们会首选逃避。你很可能会遇到拒绝参与任何修复过程的人，这并不奇怪。以下是一些可能有助于激励他们的想法。我们在手册末尾还附了一篇文章，专门讨论帮助 ★（施暴者）的策略。

如果你能找到与 ★亲近、且认为其行为极其恶劣、需要社区介入处理的人，那就安排让他们彼此交谈。表达对 ★ 的关心并让他知道你非常希望他留在大家身边。可能需要长时间的大量讨论才能让 ★ 同意处理自己的问题。如果没人与这个顽固的人亲近，就找一个至少立场中立的人去谈。

另一种策略是召集社区里的一群人（其中最好包括 ★ 的朋友），邀请 ★ 参与一场关于其行为的讨论。一定要告诉他，你关心他作为社区成员的身份，并希望看到所有社区成员都安全 —— 待人友善比严厉更有效。同时让 ★ 知道他有一系列获得支持的选择；提些建议，比如与朋友进行转化式支持、心理咨询、愤怒管理课程等等。最后，★ 可以选择与社区合作处理纠纷，或者被要求离开。

如果尽管你尽了最大努力，★ 依然拒绝与你沟通，或者他仍在实施暴力，你几乎没有选择，只能“体面地”放逐他（这可能涉及使用棒球棍）。确保将这个混蛋的事迹告知其他社区，这样他就没法在那里重

演同样的戏码。

故事 #4

小然和托尼住在一个自称无政府主义者的合作社住房里。一天，他们为了冰淇淋吵了起来，当时还有很多其他人在场。

首先，小然抱怨有人吃光了所有冰淇淋。托尼嘲笑了小然，然后小然对着托尼大喊大叫。作为回应，托尼朝小然扔了一个小木块，砸中了小然的男朋友的头。于是小然冲上去扇了托尼一耳光。这激起了托尼的冲动，他扔出了一大碗沉甸甸的燕麦粥，砸中了小然，在她的手臂上留下了一道很深的伤口。小然不得不去医院缝针。

后来，屋子里的人坐下来讨论发生的事。小然为自己扇了托尼耳光而道歉，但托尼没有为扔东西道歉。他说他认为暴力是解决冲突的一种可行方式。

合作社的其他成员认为，他们双方对发生的事负有同等责任，所以不需要采取任何行动。小然希望屋子里的其他人能站在自己一边让托尼搬出去住，但大家觉得就这样把他赶走心里过意不去，部分原因是托尼是非二元酷儿且是拉美裔，而住在那里的其他人（包括小然）都是白人。不久后小然就搬走了，因为她觉得和托尼住在一起“不安全”。

这个故事是小然告诉我的（并允许我在这里使用）。之后我问过她，屋子里的其他人本来可以做些什么，才能让她感到足够安全，从而反思自己在冲突中的责任？ 她说，首先她认为如果托尼连道歉都做不到，就不应该被允许继续住在那里。此外，她希望大家能承认暴力程度的差异。她知道扇托尼耳光是不对的，如果屋子里的人能承认托尼的行为比她扇耳光的行为“更有害”、“更危险”，她本愿意去接受咨询（或采取其他行动）。

离开虐待关系的安全防范措施

请记住，离开是这段关系中最危险的时刻。即便 ★ 到目前为止还没有实施过肢体暴力，也不代表他以后不会。说认真的，人在极端情绪下会变得具有攻击性，做出你意想不到的疯狂举动。所以，如果你正鼓励 ▲ 离开，请确保他们有支持网络做后盾。如果 ▲ 没有现成的支持网络，而你自己也没法帮他们建立一个，至少帮他们想好可以去的地方，比如妇女避难所、朋友家，甚至远走他乡等等。

以下是给 ▲ 的建议

- 如果你还在考虑是否离开 ——

如果你认为一旦你离开，★ 会彻底发疯，那么在真正行动前，考虑制定一个周密的撤离计划。

存一点钱，准备一个“跑路包”（装入备用钥匙、衣服、药品、身份证件、重要文件、电话号码和你认为真正重要的任何东西），并寄存在你信任的人那里。理想的存放地点是 ★ 绝不会首先想到去搜寻的地方。

你还可以制造些假象，让 ★ 以为你要去某个地方，而实际上你去了别处。

请记住，你从家里拨打的任何电话号码都会出现在之后的话费账单上。

- 如果你刚刚离开 ——

暂时彻底远离 ★。如果你需要回房子拿东西、和 ★ 谈话或出现在 ★ 可能在的地方，一定要带人同行。考虑找到值得信赖的朋友全程陪同（无论是陪同你还是陪同 ★）。

如果你不想让 ★ 知道你的住处，告诉别人新住址时要格外小心。

取决于 ★ 的疯狂程度，他可能会威胁那些他认为知道你在哪里的人；由于很难预料人们在受到威胁时会做出什么反应，所以你在分享信息时也要意识到这一点。

- 如果你刚刚把 ★ 赶走 ——

换掉房子、汽车或自行车的锁。

想想你和 ★ 共享的任何东西（比如银行账户、共用的暗房、学校的储物柜），并重新安排，确保你不再需要通过 ★ 就能使用它们，同时也确保 ★ 不再拥有访问权限。

考虑换一条路去学校或上班，如果可能的话，调整工作时间。

如果你没有能时刻陪在身边的朋友，申请禁制令会很有帮助。但请记住，禁制令意味着不仅 ★ 不能联系你，你也不能联系 ★。如果你主动联系了 ★，临时禁制令（TRO）就会失效。

常见的恶劣行为

大多数肢体虐待都很容易识别并确定为暴力，但其他类型的暴力则更为隐蔽。说一句“你疯了”可能和扇耳光一样具有伤害性，有时甚至更糟。言语、情感和性虐待通常更难察觉，也更容易被找借口开脱，但它们会扭曲你的大脑。我们列出了这份行为清单，以帮助被支持者和 ★（或者我们所有人）识别关系中的不健康征兆。

棘手之处在于，很多时候取决于语境和理解方式。例如，大声叫嚷在某些人看来是可接受的沟通风格；而形影不离在某些人眼中则是爱意浓厚、紧密相连的表现。不幸的是，被宣扬的“真爱”与被用来控制和恐吓的手段之间往往只有一线之隔。

底线在于：如果你感到不快乐，这就是一个信号，表明某些事情需要改变，无论你是否决定将其贴上“虐待”的标签。 身处一段关系并不意

味着对方能读懂你的心，也不代表他们必须完全按你想要的方式做事。但它确实意味着对方应该给予足够的关心去倾听，并尝试共同解决问题。如果他们不愿或没能力付出这种努力，那他们大概不值得你继续交往。这些破事儿可能极其复杂且难以理清，如果你感到困惑，可以找个好朋友帮你梳理一下现实。

行为示例

- 大声叫嚷、推搡、吐口水、摇晃、按住你不让动
- 无论去哪儿都跟着你
- 替你做决定
- 说你是个失败者、疯子、蠢货、荡妇，说没人会在乎你
- 对你的孩子或宠物很凶
- 性行为过程中拒绝采取保护措施
- 贬低你的能力
- 表现出极强的嫉妒心或占有欲
- 扔东西或捶墙
- 嘲笑或羞辱你
- 玩弄心理游戏
- 经常违背诺言

- 在他人面前批评羞辱你
- 说你不可理喻/无理取闹
- 忽视你或采取冷暴力
- 规定你的着装或批评你的外表
- 强迫你发生性行为
- 在你睡觉时与你发生性行为
- 让你证明你的爱或友谊
- 阻碍你睡觉、工作或学习
- 拿走你的钱或让你替他们偿还债务
- 身体阻拦不让你离开
- 破坏你的财物
- 隔离你，让你脱离朋友和家人
- 危险驾驶
- 以自杀相威胁
- 威胁要让你被驱逐出境（针对移民）

- 分手后的骚扰
- 让你相信这一切都是你的错

报警

我们都知道，警察及其系统是腐朽不堪的。编写这份手册的主要原因之一，就是鼓励人们寻求基于社群的解决方案，以避免报警。但这并不总是行得通，你可能会面临警察是唯一可行选择的情况，可能因为社群支持系统尚未建立，或者你无法获得。

如果你的生命受到即时威胁，可以报警。 哪怕警察无法及时赶到（或者到了也帮不上大忙），但他们的出现有时确实能防止你在那一刻受到伤害。

如果你有受虐待的身体证据，无论你是否希望如此，★ 都有可能被逮捕并关押几天。反之，即便你希望带走 ★，警察也可能无动于衷。如果你起诉，你们双方都会卷入司法系统，不得不应对强制性的出庭日期和繁琐的官僚程序。★ 可能会被处以重罚，并被要求参加愤怒管理课程。

请注意： 如果任何一方或家庭成员是所谓的“无证移民”，牵扯警察会使他们面临被驱逐出境的风险。此外，有色人种、酷儿或跨性别者，始终面临更多遭遇警察暴力或不公审判的风险。

另一种法律途径是申请禁制令。但这并不总能阻止施暴者，警察也不会随时待命保护你。

总之，只有你才最了解自己所处境况的真实现实。不要为了保护 ★ 不受体制惩罚而冒生命危险； 但也不要指望这个体制会真心支持你。

故事 #5

我曾帮助好朋友道恩摆脱一段充满暴力的关系，当时她正在和社群里的另一个女人安娜交往。她们决定一起旅行并搬到一个新城镇。离开后，我经常接到道恩的电话，她向我描述安娜如何对她发疯并殴打她，有时甚至打得她鼻青脸肿。我和道恩谈过分手的事，但她说她离不开，因为安娜在金钱和生活上给她提供了帮助。这样持续几个月后，她们终于分手并分开住了。

然而之后她们又开始旧情复燃。一天晚上，道恩喝了几杯酒后去了安娜家，发现安娜正和另一个女人在一起。道恩就发疯了，她推搡安娜并开始对她尖叫。道恩拒绝离开，并在对方尝试报警时拔掉了电话线。最终道恩离开了。

随后安娜对道恩申请了禁制令。道恩对此极其愤怒，因为以前她曾无数次被安娜殴打。令她气愤的还有，安娜虽然自诩为无政府主义者，却利用法院系统来对付她。

安娜是在利用禁制令威胁道恩（因为道恩从事青少年教育工作，禁制令会影响她的职业），而且安娜明知道道恩在法律上被禁止联系，却还继续主动联系道恩。最终，道恩也申请了类似的禁制令，后来她们一起出庭并决定撤销双方的申请。

此后她们分开了一段时间。接着她们又恢复了朋友关系并开始上床。道恩并不想真正复合，且当时正与别人交往。当安娜发现后，她威胁要自杀，表现得极其崩溃。

现在，道恩已经搬离了她们原本居住的城镇，因为安娜所有的朋友都在监视道恩的一举一动，或者因为听信了安娜的一面之词而对她态度恶劣。

[image]

这个情况极其复杂，没有一个绝对清晰的“坏人”。由于双方都向各自的朋友诉说，这件事对整个社区产生了很大影响。这种涟漪效应甚至波及了好几个社区。

这两个女人都有着某种相似的行为模式，这将继续影响整个圈子。

健康的关系应该是什么样？

一段美妙的关系应该是让你能够：

- 公开表达你的感受、想法和渴望
- 追求你真正想要的生活目标
- 共享时光和经历，感受彼此的陪伴
- 共同面对和处理关系中的难题
- 公平地协作以寻找解决方案

结语

对所有坚持读到这里的朋友说：太棒了，干得漂亮！我们没有更多的微言大义了，已经倾囊相授。但我们有很多的鼓励。我们知道，有些针对创伤的建议是一种理想化的愿景；所以，请根据你所在的社群/圈子或所处的具体情况，去打磨它们、重塑它们、给它们印上你喜欢的烙印，并灵活运用。

如果您有任何进展，请告诉我们。我们始终乐于接受并渴望得到反馈，但我们并不打算开一家咨询公司，我们不是专家，也不想成为专家。这个过程取决于你如何塑造它，我们不承诺它会百分之百奏效。但我们知道你们所有人都很棒，你们的社群有能力处理这些破事儿。

[image]
[image]

S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放

[image]	关键词	
[image]	创建时间	2025年10月1日
[image]	**Description**	关系结构革命

[image]

构建亲密关系是一项顶级能力。是这个变革时代最至关重要的能力。

是区分口炮异议和革命者的关键标准。

停止幻想所谓的“灵魂伴侣”。

灵魂伴侣不是缘分造就的，而是我们反抗这个鱿鱼世界的成果。

[image]

[image]

建设中！敬请期待。

[image]
[image]

性、婚恋、密友…“反贼”如何构建亲密关系：战友爱侣S10E01

[image] 关键词	
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月2日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

杀猪盘和可利用的同理心：战友爱侣S10E02

[image] 关键词	
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月3日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

亲密关系中的权威主义：战友爱侣 S10E03

[image] 关键词	
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月4日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

所谓的“开放关系”可能并不是你想的那种…：战友爱侣S10E04

[image] 关键词	
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月5日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

关系无政府状态的伦理学：战友爱侣S10E05

[image] 关键词	
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月6日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

无界，无级，无限，无尽 …… 无忧，自带安全感的亲密关系：战友爱侣S10E0N-1

[image] 关键词	亲密团队 人际安全 关系 关系结构 团体 心理安全 爱
[image] 关联	[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月30日
[image] **Description**	关系结构革命

你体验过那种亲密无间的关系吗？毫无顾忌地坦诚相待，成为彼此的情感支持，信任和依托 … 这就是我们常说的”亲密关系”本该有的样子。

这里完全不考虑性、无所谓任何”性别”，也不会把情感详细地分门别类。

只说关系本身为您带来的感触 - 那种自然安全的、带着鼓励的积极，沉浸在这份关系中可以让你感到更有勇气迎接挑战，更自由，更纯真，从而更有热情和好奇心去尝试更多新东西；

更少疑惑，不再需要小心翼翼，不再需要筑起高墙来保护自己 ……

不再抱怨和自私，享受那种发自内心的延展感和自在。

如果你能在爱侣关系中实现这一层次的亲密，你就能把这份经验复制到更多友情关系和协作中，摆脱圈子江湖，打破商品社会强加的工具性人际关系结构，创建自己的 亲密团队 。

[image]

那，究竟可以怎么做？也许没有一个细致入微的且普遍适用的教程。但我有一些私人经验，愿意分享给你。也许能让你有共鸣，如果更好的话，也许还能点亮你的灵感，帮你开拓出更多新方法。

下载可打印版杂志：

https://drive.google.com/file/d/1r1zx_PdIsjWaZezxzaPGx07_y8y3fWZW/view?usp=sharing

[image]

普通的恋爱关系大致都遵循这样的模式：起初，你遇到了一个美丽的新人，你们彼此开拓视野，共同经历美好时光，从而坠入爱河。

在开始阶段里，你们的共处时光可能比任何其他时候都能让你感到更加自由，世界似乎充满了无限的可能性和狂野的喜悦。

但渐渐地，你们不再信任外界世界，开始对最初那份美好的未来可持续性产生怀疑。

为了挽救它，你将关系筑成了一座堡垒，以阻隔寒冷危险的”外部世界”，并通过将激情转化为制度来保护它（你只能跟我玩！我不管，就不，你必须顺着我！…… 你为什么允许那个人跟你开那样的玩笑？你心里还有我吗？……要是下次再让我看到你跟她说话，我就……）

性，最初是比任何事物都更自然、更自由的存在，你们对彼此身体和感触的探索和好奇心曾经给你打开了一片广沃的新天地。但却逐渐地，性事被当成了守护爱情关系的圣物，成为了证明你俩的关系与其他关系”不同”的证据。（回头想想都会感觉奇怪，这是性所扮演的最

畸形的角色）

不可避免地，有一天你会醒过来，意识到曾经将我们团结在一起的那些自由的、野性的激情已经消失，取而代之的是习惯、是常规、是对变化的恐惧。你为了保护爱情而建造的城堡，如今已经变成了一座坟墓，将你和伴侣封闭在里面，与外界隔绝。而实际上你们一直需要外界带来新的事物，以供彼此分享、并维持自我。（甭管7个月还是7年，早晚都会”痒”，早晚都会”腻”。”新鲜感”一过情人就变仇人……智者不入爱河……）

在”棺材”里，你们越来越频繁地争吵，彼此都在要求对方牺牲更多来”证明”爱意 —— 而爱本应让你活得更好，而非以”基本陪伴的保证”为代价让你陷入瘫痪。你有没想过，这种”陪伴”往往只是意味着剥夺了你参与更大社群的可能。

坠入爱河曾经让你感到如同发现了通往伊甸园的秘密入口，一个可以摆脱社会上无处不在的工具性和竞争性人际关系的疲惫的大好机会，享受到无需计较得失的、无需担忧“公平交易”的馈赠经济；但如今，你们又回到了交换经济中，竞争着看谁依赖性更大、需要对方更多，谁能掌控对方更多。你的伊甸园已经被鱿鱼游戏的毒霾覆盖。

[image]

为了超越浪漫关系中的刻板角色定位你进行了很多努力的尝试，然而你突然发现，自己又成了所谓的“男朋友”（在这种性别歧视的社会中，任何人都不该被迫扮演这样的角色！），被“女朋友”塞进严格的”好男友”模具中，塞不进的部分被扔进名为”渣”的垃圾桶里。你开始感到惶悚不安，原本最亲密安全的地方现在变成了最危险的地方，却完全不知这一切是如何发生的。

你开始思考，为什么总是陷入这样的模式，下一次怎么办？可以避免吗？如何 ……

关于限制的问题不断浮现，即 某些事情似乎必须被排除在外，关系才能正常运转。（我不能这样，也不能那样，否则*TA*就不爱我了…）

与朋友相处时似乎更简单些，没那么多禁区，也没什么要求：朋友间彼此给予力所能及的帮助，在有能力给予时给予，且不会强求对方做不自然的事情（至少在健康的友谊中是这样）。

到此，你会像我一样，开始决定探索其他爱情关系模式，发现确实存在一种没有这些限制和期待的关系传统：非一夫一妻制的关系，或者说，“开放”关系。

请注意，我并没有在说一夫一妻制关系是坏的，但关系形式千千万万，而我们通常只允许自己尝试一种模式，这似乎很荒谬。不如来探索一下不同的可能性。

每当我听到另一位妻子/丈夫/男朋友/女朋友偷偷摸摸地出轨时，每当我听到有人自豪地谈论如何（以一夫一妻制的名义）成功抵抗了做某件事的“冲动”时，每当我不得不听着某人可怜巴巴地抱怨自己被“困”在一段关系中、或因某种恐惧而无法追求自己的真实欲望时，每次我不得不目睹所谓的男凝甚至偷窥时（“只要不碰就没事”，对吧？），都让我对人们如何将自己困在这类单一选择的关系体系中感到愤怒。

大多数人已经接受这些令人窒息的症状为”不可避免”，而不是去探索其他可能性。

最重要的是，对一夫一妻制作为唯一选择的执着（除了随意的一夜情吧，那也无聊至极且在其他方面很有问题），让你我无法坦诚相待。

我们必须敢于直面生活与欲望的复杂性，即使这会带来痛苦。

♡

作为朋克摇滚乐迷我们总是自诩为激进分子，但当真正付诸行动时，尝试那些与我们的革命理念更契合的截然不同的或者具有挑战性的生活方式时，我们中很多人从未质疑过自己已经被程式化的习惯。我们的革命思想往往只是一枚徽章，是我们用来投票的不同意识形态，而非改变生活的催化剂。这背离了我们理应作为示范者和开拓者的角色。

这是一个影响每个人的问题，无政府主义价值观可以在现实世界中得到尝试，但到目前为止，我看到我们社区中对此主题的讨论非常少；如果我们要质疑世界运行的方式，我们应该将这种质疑带回我们自己的个人关系中，或许先在我们自己身上尝试替代方案，然后再提出解决世界问题的方案。换句话说 —— 如果我们真的有解决社会问题的方案，那就先将这些方案应用于解决我们自身关系中的问题。医人先医己。

[image] [image]

开放式关系究竟是什么

这里最重要的是要摆脱这样一种观念，即：认为一个人的价值取决于他/她是否能独自成为另一个人“足够充分”的伴侣。就像毒鸡汤所言“只要你保持住完美，对方就不会离开你”。这非常荒唐。

世界是无限的，我们每个人也是无限的——无论我们活得多么充实，与他人互动的次数或深度多大，都不应成为任何人“足够充分”的标准，正如与所爱之人互动的次数或深度，也永远不会成为“足够”的标准。”（对他人能做或感受的事情设定界限，作为他们获得我的爱与关怀的”条件”，这与我作为无政府主义者和普通人类的信念背道而驰；我愿意相信每个人都知道自己需要什么，于是我从不限制别人 —— 当然也绝不认为对他人设限会让我自己的生活更加丰富。）

我们必须解放彼此，让彼此成为/（发展成为）真正的自己。这不仅关乎其他恋人、性伴侣、或朋友，也关乎其他追求、需求，甚至对空间与独处的渴望。令人心碎的是，我们的恋人常常要求我们为与他们相伴而牺牲多少自我。

我希望被认可的，是我的本真，是我天生具备的能力，而不是我有多么符合他人预设的需求清单。如果其他任何人能满足我的恋人的部分需求，我不会剥夺那个人的机会，我也不想在看到别人拥有不同于我的东西时感到嫉妒；我只是希望有机会将我所能给予的奉献给所爱之人，并记住这些东西是无价的，无法与他人独特的礼物相提并论。

无论如何，我们都不应被赋予成为他人需求”唯一提供者”的角色（无论是浪漫的还是其他方面的需求）；我们在地球上的目的不是为了服务他人，而是为了找到方式成为自己，同时也能造福他人。当你真正认识到世界其他地方对你的伴侣来说并非禁区时，你就解除了自己成为伴侣”整个世界”的责任。

一夫一妻制意味着人们在某些方面会犹豫不决，不敢与他人分享自己，害怕陷入暧昧 —— 因为你被责令一次只能有一个恋爱对象。也因此，该制度下的人们不得不确保所选择的唯一伴侣是”一笔值得的投资”。男人们疯狂捞钱、健身、沽名钓誉，女人们一掷千金做整形手术，只为加码”性资本”，把自己卖个好价钱。

于是由此，显而易见的，你又回到了抠索算计的资本主义市场博弈关系结构之中，连你的恋情也被它吞没。

女性会评估男性的经济能力，男性则会思考女性的颜值是否足够”达标”以致于带出门去能给自己添面子。没有人愿意与那些不符合这些标准、因此”不配”成为潜在配偶的人尝试亲密。

同样地 —— 就像在友谊中一样，世界上可能有这样的人，你可以与他们每月共度一两次美好浪漫的时光，但你们之间缺乏足够的共同点来维持稳定的恋爱关系更无法组建家庭（尽管你经常看到这样的不匹配夫妻，他们本可以作为偶尔的伴侣而过得幸福安逸，却在五十年的婚姻契约中被绑在一起彼此折磨）。

非一夫一妻制的关系使自主幸福成为可能，而无需付出相互折磨所有人都不幸福的代价。

[image]

我决定不再在友谊与爱情关系之间划分价值等级：它们在我生活中同等重要、不可替代，任何想让我在它们之间做出选择的人都滚蛋吧。不仅如此，我已经不再根据一些任意的表面细节来区分“爱情”或“友情”—— 我与某些朋友分享的感情是如此亲密、如此美好，仅仅因为我们之间没有发生过性关系，就不能称彼此为"恋人"？这简直荒谬。将性行为作为划分彼此间关系界限的标准，决定哪些关系优先，决定我们与谁玩乐、与谁同住、与谁共眠、谁是我们"首先应该照顾"的对

象、谁是我们最终与之共赴黄泉的亲人，这简直荒谬至极。

同样地，在开放关系中，性行为不会被赋予如此多的含义和限制。在当前社会中，超越一夫一妻制模型的爱与欲望被妖魔化并遭到全方位攻击——至少在女性的生活中尤其如此，而那些不愿一夫一妻制但又厌恶“一夜情玩家”圈子的肤浅和性别歧视的男性，也很难在女权主义圈子中找到支持。性不应被束缚，也不应被赋予任何象征意义—— 性仅仅是人们彼此之间以身体方式表达亲密、给予愉悦、实现情感交流的诸多方式中的一种，双方应平等承担参与责任，无需向某些过度挑剔的群体、社会期待或道德禁忌低头。

开放式关系就是这样：它是一种”关系”，其中人们可以彼此坦诚相待，也可以坦诚面对自己 —— 在这种关系中，无需隐藏、没有压抑、不会设限，整个世界都可以成为你我探索的对象，无需担心触碰虚构的界限。

如果你在包含界限与禁忌的关系中要求彼此完全开放与诚实，那实际上只是在为背叛与不诚实埋下伏笔：若只喊出“要开放！” 却对所有可能的真相缺乏接纳，这种态度既专制又荒谬。

若想让真正的诚实成为可能，我们必须在彼此个性的每个层面都给予支持。否则，就像基督徒那样在告解时互相要求出于某种道德义务去揭露一切，却随时准备用羞耻的鞭子惩罚任何偏离的冲动。

我们必须学会接纳并庆祝任何让彼此感到愉悦的事物。如果对爱侣有益，对我们就也有益—— 真的会有人如此自私以至于完全看不到这一点吗？

你和朋友们组团旅行过吗？以此为例，来理解这种关系的运作方式。在旅行中，不同个体建立了紧密的联系，很可能像恋人一样分享私密世界；但他们也记得，为了让团体活动正常进行，每个人都不能从与他人的关系中抽身。每当两个人需要彼此休息一下或希望拓展视野时，他们会花更多时间与其他人相处，因为周围总有其他人也能提供价值。每个人都感到安全和被关怀，没有人被排除在外，因为我们并没有被配对成排他性的二人组。

相反，我们当前所处的恋人稀缺性经济，使得每个人都急于挑选另一个人、急于宣示主权、并将其束缚住，生怕被遗弃，似乎一脱手就永远失去了。而这种对孤独的恐惧使我们无法看到的另一种选择，似乎更具吸引力的选择：一个没有边界的世界，其中我们每个人都将成为一个更广阔的恋人与朋友的大家庭的一员，恋人与朋友之间没有区别—— 也没有任何关系必须遵循固定的模式，因此实验性将成为每段关系的常态，故而，没有任何关系会变得枯燥或令人窒息。

要达到这样的世界，我们只需习惯于不限制彼此，不将”爱”视为一种有限的资源。

[image]

嫉妒，以及我从中领悟到的道理

是的，我偶尔还是会感到嫉妒。过去我曾经历过极度嫉妒的时刻——不仅是对其他男人的嫉妒，还包括对伴侣所热爱的、经历的或感到兴奋的其他事物的嫉妒。能够接受这些情感对我建立自信和自我认知至关重要。

我花了数年时间才真正体会到（而不仅仅是理解到），如果我的伴侣也爱其他事物或其他人，这并不意味着我价值较低"被比下去了"。况且，如果对方真正爱我，那并非因为我符合某份理想品质清单，随时都有可能出现任何新人比我做的更好、更符合标准，那意味着我"需要"持续处于恐慌之中吗？……不。

我被爱，是因为我的独一无二的特质，这是没有任何人能与之竞争的，所以我无需恐惧。爱并不是稀缺的商品——它是会成长会不断增加的价值，就像快乐一样，越是被允许、被分享和赠予，就越会增长。

我现在不再觉得必须把某人完全据为己有才能满足"安全感"了。我知

道这样做行不通，尤其是，这样做法传递爱 —— 或者说无法传递我本身。

我认为我的嫉妒是一个值得直面的对手，如果我真正去直面它而不是试图通过控制他人来保护我自己，这份嫉妒情绪就能让我更多地了解自己。我之前在关系中曾有过这样的经历：我的伴侣为了保护我免受嫉妒的困扰而限制自己，这对我们双方都造成了灾难性的后果，你可以想象。如今，我认为帮助他人不再“为我担心”与我学会不再为自己担心，同样重要。

嫉妒让我明白的一件事是，我对其他男性的态度。有趣的是，我从未因伴侣吸引或涉及的女性而感到威胁，但其他男性总会让我怒火中烧。在我们的社会中，男人们被灌输的是不要信任彼此、甚至要憎恨彼此、要永无止境地全方面竞争、要试图“保护”女人免受其他男人的侵害（这往往更像是囤积和守护“财产”），当你看到许多男人在与女人的互动中有多么扭曲时，就能理解这点了。

但对我来说，不信任任何男性能为我的伴侣带来好处（超越有限友谊的范畴），这纯粹是偏执和领地意识的昏头症状。

如果我信任伴侣的判断力，就应该相信她知道什么东西和什么人对她有益，而 不让 那种“人人为敌”的男性条件反射干扰我的判断。

[image]

我听到过的一些关于’开放式关系’的反对意见：

> “听起来不错，但人们的感受比这些抽象概念更重要……”

有些人认为，我们这些知识分子式的提出想法和理论的人"并非"为了解决生活中真实存在的问题，而是为了"炫耀"自己能想出多么好的点子。如果到现在你还没明白，我是在试图解决而非加剧我自己的恋爱

关系中的问题，那我为前面所有文字的失败而道歉。而且，如果你觉得开放式关系会对你的情绪造成压力，那就试试长期一夫一妻制吧。两者都有其艰难的部分。

> “但人性——”

拉倒吧。不必多说。人性是我们塑造的，而你心里也清楚这一点，无论你是否愿意承认——你们这些胆小鬼、找借口的混蛋。

> “我想如果这是你想尝试的，那随便你，但幸运的是，我只想要一夫一妻制！不管怎样我准备好了！”

这对你来说很好，如果这是真的很好的话 —— 至少目前是？当我们的欲望恰好与社会规则相符时，总是会感到欣喜若狂；那时，我们很容易为自己的欲望感到自豪，认为它们是如此美丽，因为它们被普遍接受（事实上，你周围的一切都在强化这样一个观念：你此刻有幸感受到的正是完美本身）……但你可能并不总是那么“幸运”，你知道的。如果你（或他人）有一天感受到了单一伴侣制无法满足的欲望，而你尚未努力让他人理解并认可存在多种可接受的关系与欲望形式，你将被迫回到起点，发现自己被误解、被憎恨，被冠以淫娃荡妇破鞋之名。

没有人应该经历这种事情，所以，无论你个人需要什么、你眼下需要什么，你都有责任推广非一夫一妻制作为一种可行的选项。否则，包括你在内的每个人都将生活在恐惧之中，担心某天醒来时会产生一种不可接受的欲望 —— 而这种道德主义对我们生活的法西斯式控制，正是我认为我们在朋克摇滚中试图对抗的东西。

这就是为什么我目前认为自己是非单一伴侣关系者，尽管过去五个月我只与一个人发生过性关系：我所做的一切并非出于对单一伴侣关系的承诺，而是出于对满足自身需求和他人需求的承诺，我的选择跟社会规范一点关系都没有—— 并且支持那些做同样事情的人，无论他们是否以相同的方式去做。非一夫一妻制与性无关 —— 它是一种与人建立关系的总体态度，即：无主权、无支配、不控制、不操纵、不设限，从而不焦虑不担忧。如上所言。

> “ 开放式关系对女性不利 —— 这只是给了男人不负责任的机会 ……”

这是我宁愿不必面对的性别歧视言论。但我之前确实听过类似的说法。这让我想起那个陈旧的迷思：所有“好女人”都渴望“负责任”的专一关系，而那些不追求专一的女人必定是没脑子的（因此是值得怀疑和鄙视的，就像那些厌女症患者称她们为破鞋一样）。

首先，正是女性向我介绍了关系结构革命的观念。除了我认识的女性，我能找到的关于这个主题的最佳书籍（《道德荡妇 The Ethical Slut》，作者是多西·斯顿和珍妮特·哈迪， Greenery Press 出版），强烈推荐给对这个话题感兴趣的人。其次，过去几十年间参与开创不同关系模式的许多男女并未涉及异性恋关系，因此在这些情况下，这种批评完全缺乏依据。第三—— 这么说的人似乎认为，男性只会对那些用性行为作为”报酬”的女性给予情感关怀 …… 并通过剥夺她们获得其他性享受的机会来确保这种报酬机制始终有效。天啊，你期待的异性恋结果就是这样吗？

最后—— 是的，男性确实被社会化成了自私自利无情无义的模版，仅仅改变人际关系模式并不能解决这个问题。但这在任何类型的关系中都会成为问题，而不仅仅是爱侣关系。这个问题必须作为独立问题来处理。

一个充满爱与关怀的男孩不会在恋人（或其中一位恋人）真正需要他时，跑去与陌生人发生性关系。

我们的性欲中隐藏着太多地雷，因为其中大部分已被我们的敌人编程，被编程为害怕真诚而不是享受贴心、恐惧动情而不是享受停靠的归属感。咱们这些男人需要主动摆脱那些迫使我们通过追求肤浅的性行为来逃避真正的亲密与支持的压力。

这让我想到另一个反对意见：

> “那是否意味着你放弃了你的浪漫梦想，放弃了你幸福生活的希望，只是用它们换取与熟人的一系列性

事？”

不，完全不是。我并不想逃避个人承诺和长期关系 —— 相反，我希望保护我的关系免受不必要的风险。我希望巩固我的恋爱关系，让它们不会因一些琐事，比如暂时的无聊或对他人偶然产生的好感而受到威胁。我希望建立能够适应我生活和需求变化的可持续关系。这样，我就能与我的爱人相伴就像与朋友相伴一样，直到死亡将我们分开，而没有旧的禁忌（或嫉妒、不安全感等）来干扰。

当然，这有时会很困难，就像生活中的一切有时都很困难一样—— 但我认为，这样做的回报在各方面都会更大。

我希望在这里做的是，让我们摆脱爱情关系中不必要的悲剧，摆脱那些阻碍我们获得承诺和快乐的不安全感和占有欲。为了准备好移除这些障碍，我们必须准备好以极大的勇气直面真正的悲剧：我们不能要求他人通过限制自己来保护我们免受不安全感的困扰，我们必须面对这样一个事实，即 会有某些时刻我们是孤独的。不这样做的代价是荒谬的 ——今天，我们在关系中承受着各种必要和不必要的悲剧，只因我们缺乏勇气。这种情况下激励自己去尝试点儿新事物，难道还有什么过分的吗？

[image]

By Crimethinc

[image]
[image]

构建没有内耗的爱：把我们的亲密关系从资本主义逻辑的泥潭里拯救出来 - 战友爱侣S10E0N

[image] 关键词	人际安全 关系 关系结构 反叛 团体战术 无政府主义 爱 组织 资本主义
[image] 关联	；[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2025年10月31日
[image] Description	关系结构革命

"We love the things we love for what they are." ~ Robert Frost

- Table of Contents
下载手册，可打印：
资本主义的逻辑
以结果为导向的关系
以过程为中心的亲密关系

[image]

下载手册，可打印：

https://drive.google.com/file/d/1tmIvtCV_nuujQgfuzoWM8ZdflQ0f1zhN/view?usp=sharing

怎么一谈恋爱就内耗呢？难道我们建立亲密关系不是因为想要追求快乐吗，却为什么越爱越痛苦？…… 当最亲密的关系受挫，所有社会关系都会变得诡异，令人疲惫。协作能力每况愈下。甚至草木皆兵……怎么办？

的确，亲密关系的成功可以带来显著的信心和勇气（以及底气），反之则可能导致安全威胁。在风险行动中，爱是一件强大的武器，培养、处理和维护亲密关系的能力，对革命者来说至关重要。这就是为什么我们将相关内容中侧重于方法(战术)的部分放在本站中。

这方面没有简要的通用的教程，很大程度上需要您通过实践来摸索—— 去谈恋爱。（注：谈恋爱不是搞对象哦，这是两件事。前者是协作，注重平等共进无主权；后者是适配，很可能带有支配性和控制性。）但仍然有一些原理和他人的经验，值得您了解。

[image]

资本主义的逻辑

今天反抗资本主义的人们回顾上个世纪反资本主义的重要著作时，就会发现，许多看似清晰且持续具有现实意义的著作中都存在着一个共同的缺陷：他们认为“资本主义的终结迫在眉睫且不可避免。他们认为资本主义的强大在于其压迫性力量，而这种僵化的、压迫性的力量终必然会因为无法维持其形态而崩溃。

然而前人们未曾预料到（我们如今已然明了）资本主义具备惊人的适应能力。其非凡的持久力不仅源于压迫性力量本身，更在于它能让如此之多的人们甘愿成为维护该体系的基层执行者，而该体系恰恰损害我们所有人的利益、毒化我们的社区、并导致我们彼此间的关系难以维系。

[image]

资本主义得以长命，不仅因为有权贵阶层在强制执行它，更因为，我们其他人已经将其逻辑内化了，在日常生活中遵循其节奏。这种资本主义逻辑是：始终生活在对未来欲望满足的承诺之中。我们不仅在通常被视为资本主义逻辑的领域（如工作场所、选举政治等）中践行这一逻辑，更在最亲密的人际关系中践行它。后者正是本文即将深入探讨的领域。

作为人类，我们天生就带着一种内在的失落感。我们必须面对的失落不仅在于我们的生命、以及我们所爱之人的生命，都是有限的，还在于，我们生活在一个无法完全理解的宇宙之中。在这份失落感中蕴含着巨大的创造潜力—— 艺术、游戏、社区、信仰、哲学 —— 但要与这份潜力建立联系，就必须接受并直面失落。或许没有什么比直面失落更艰难、更痛苦的了（而从某种意义上说，也没有什么比这更令人满足或充实的了）。

这种内在的人类失落感以多种方式显现，但很少有比我们创造语言、命名事物的能力更清晰的体现。当我们为一个事物命名时，就同时创造了超越该事物本身的东西，而我们对物质的渴望正源于我们无法真正满足于它。符号是无尽的、抽象的、非局部的，而它们所指代的物质具有有限性，而在这两者之间的无桥之境，正是我们的失落感与欲望的并存之处。

资本主义的逻辑察觉到了这种失落 —— 真实现实与符号现实之间的鸿沟 —— 并试图通过消费来填补这一空虚，以避免失落的痛苦。

总有另一款“新”产品面世并承诺带来极致的满足感、告别所有遗憾。然后你马上就会发现，最新款的 iPhone 并没有如预期或希望的那般带来满足，它并非是我们追求的完美对象，但“别担心，下一款 iPhone 或许就能满足你的所有心愿了”。无论是自觉的还是不自觉的每个人心里都清楚，这种逻辑中有明显的悖论。即便理论上能提供终极、完整的满足感，资本主义也无法实现它 —— 因为这将意味着资本主义与消费本身的终结。这是资本主义永远无法兑现的承诺。

然而，它仍在人们的思维中播下了其逻辑的种子：终结失落、痛苦和匮乏的可能性。但是它永远只能存在于遥远的天际线彼端。我们的满足感 —— 我们摆脱欲望的自由 —— 总是似乎远在天边，却又令人垂涎地近在咫尺。

对“更美好未来”的承诺。

正是这种逻辑，导致我们即便了解资本主义的运作机制，在对其反抗的过程中仍会发现自己被困于其中，它也渗透到了我们自己的哲学里。当我们在理想的反抗蓝图下承诺一个“更美好的未来”时（即终极

满足感），我们就已经将这一承诺变成了我们自己的抵抗模式，我们也踏入了资本主义的竞技场。解放不再是我们此时此刻可以采取的行动，权力不再是我们今天生活中可以承担的责任，而是变成了遥不可及的目标。

[image]

以结果为导向的关系

虽然在所有斗争领域都能找到这种逻辑的例子，但本文将探讨的是它在我们的亲密关系中的具体表现。

我们许多人从小就被灌输这样的观念：关系是实现幻想的可能性（“当我找到一个我深爱的人，然后结婚，然后买房子，然后生孩子，然后养育这些孩子，然后然后然后……”）。我们常常沉迷于对未来生活的幻想，执着于试图将他人融入这种预设的模式，以至于完全忽略了彼此的现实。将这种资本主义逻辑内化后，问题变得尤为棘手，因为我们开始依赖它来获得幸福感。即便在几乎不可能的情况下，你真的过上了梦寐以求的生活，它也无法带给你满足感，仅仅因为你始终只知道将幸福感寄托在遥不可及的“未来”，而非当下所在之处。

同时，这种逻辑还导致我们把他人视为实现我们个人愿望的工具，而非他们本应具备的主体性。当我们沉迷于为关系设定未来目标以使其变得“有意义”时，就已经不可避免地错过了关系中最珍贵的部分：那些渴望与我们并肩而立的真实、独特、完整的人。

当我们专注于未来（且真正不可知）的结果时，我们就会错过当下过程的丰富性。我们就错过了见证我们所爱之人成长为他们自己的机会。我们就会陷入试图控制这种成长的恐惧反应中，从而错过了支持这种成长的喜悦。

将亲密关系中的对方视为实现“我”之幻想的工具，就剥夺了对他们人性完整性的尊重，而且还将其物化了。意味着赋予他们“价值”的依据不在当下，而在于他们能否承诺给我们“未来”—— 永远都是未来

—— 的满足感。这符合资本主义的矛盾逻辑，而这种承诺是无人能兑现的。例如：如果我们在关系中看重的是它能持续一生（避免失去的痛苦），那么满足感只能在某人去世的时刻真正实现，即承诺的完全兑现。然而，当我们站在所爱之人坟前时，有谁会说这段关系中意义最深远的方面是合同的完成，而非那个人本身为我们的生活带来的独特精神？此外，即使是这份契约成立，也只能在有限的时间内保护我们免受失去的痛苦：任何经历过至亲离世这种深刻损伤的人都能证明这一点。

本节尾注：回想一下你三年前、五年前或十年前对未来生活的幻想。它是否
全按照你想要的或预期的方式发生了？更重要的是：你有多庆幸它没有按照
预期的方式发生？

[image]

以过程为中心的亲密关系

[image]

在资本主义逻辑的浸润下，我们如何才能建立当下的、非交易性的、且令人满足的亲密关系？我们如何培养彼此之间的关系，使其能够具备可持续性，同时避免陷入对未来结果的承诺或保证的期待中？

尽管资本主义逻辑许下诸多承诺，但并不存在完美关系的公式。在拒绝这种逻辑时，我们甚至可以庆幸：完美关系没有公式可言！最后，我们可以开始探索哪些关系对我们有益，哪些关系能促进相互尊重与责任感，哪些关系在当下对我们具有价值，以及哪些关系能让我们茁壮成长。

摆在我们面前的最大任务是找出资本主义 - 以结果为中心的逻辑 - 如何模糊我们在亲密关系中的价值判断。

以下我将列举一些问题，我个人在问自己这些问题时受益良多，尽管这绝非一份全面的清单：

1、如果这段关系明天结束，它今天对我来说是否仍然有价值？

2、我与TA在一起是因为TA这个人本身吗（而不是TA的任何身份），还是因为我认为TA能给我带来什么？

3、如果这个人决定想要与我建立不同类型的关系，我是否仍然会珍惜TA？即使我发现自己无法给予TA想要的不同类型关系，不得不分道扬镳？

4、我是否因为担心失去这个人，而对TA的其他类型的关系感到提心吊胆？

5、 我该如何调整我的关系价值观，让自己基于自我价值而感到踏实，并为所爱之人拥有其他关心他们的人而感到快乐？

6、我怎样才能面对自己内心对失去的恐惧，而又不要求与我有关系的人做出结果承诺？

7、我喜欢这个人的哪些方面是完全独立于他们为我所做的事情的？

8、 我想要从关系中得到的东西是否公平、公正和善良？

9、我向关系中的伴侣提出的要求是否尊重他们的人格完整性与自主权？还是我要求的事物需要对某些方面的控制？

当我们自问这些问题时，就能开始理解我们为何渴望关系、我们的期待是什么，以及是否存在需要我们反思和挑战的价值观。

关系这一话题具有极强的私密性，即使是对那些习惯于质疑根深蒂固的假设的反资本主义者而言，我们也容易将自己在关系中展现出的行为方式归结为难以捉摸的个人偏好，或者“事实如此别无他法”。但那些研究权力领域并试图颠覆它的人应该知道，权力的范围不仅存在于国会大厅，也不止于工作场所的边界，而是延伸到我们生活的方方面

面：包括且往往尤其包括我们彼此间的关系。那些习以为常的、被期待的、难以质疑的事物，并不一定对我们有益，往往需要最严格的审视。

将我们在关系中持有的价值观从以结果为中心转向以过程为中心，摆脱资本主义逻辑，是一项艰难而复杂的工作。最重要的是：这是一项深刻的个人工作。我们许多人被教导认为，我们的生活和亲密关系只有在产生某些“结果”时才有意义。资本主义异性恋父权制告诉我们，拥有配偶、抵押贷款、子女和孙辈都是“成功的标志”，并为那些希望按照不同价值观生活的人设置了粗暴的结构性障碍。仅仅重新包装一个新的“自由恋爱”运动是不够的，因为许多人实现经济稳定的唯一选择似乎需要一种以结果为导向的关系模式。

在人际关系中拒绝资本主义逻辑需要双管齐下的方法：一方面要进行往往痛苦且始终困难的自我内省工作，学会以自我为根基（而非将自我价值感外化为他人对“我”的看法或愿意为“我”做的事）；另一方面，要努力 构建社区支持网络 ，以提供个人稳定性，从而培育以过程为中心的亲密关系。

有人可能认为，在存在诸多结构性障碍、难以建立真正以过程为中心的恋爱关系的情况下，我们不能指望人们去做艰难的人际关系工作：我们必须先废除这些结构，然后再解决人际关系问题。但这意味着重新陷入了一直在污染我们的资本主义逻辑。如果只能等待完美条件来实现重要的人际关系工作，那就将永远处于等待状态，在等待过程中在未来世代中重复相同的适应不良的亲密关系价值观。

虽然假装重新思考、重新评估和重新构建我们看待和实践关系的方式并非难事（的确是），但忽视我们开始这项工作的原因将是一个更大的错误。我们这样做是为了开启欢乐的可能性。以过程为中心的关系观本质上是关于沉浸其中。当我们与所爱之人建立联结并融入社群，且拒绝让自己陷入对“结果”的期待与强求时，我们就能真正沉浸于关系中最美好的部分：见证彼此。我们能够体验到以真实健康的方式成长的喜悦，也能够见证和支持我们所爱之人也拥有同样的成长。我们有可能同时找到自主性和安全感，而不必为了其中之一而牺牲另一个。我们能够享受彼此共同创造的乐趣，爱将成为一份珍贵的礼物，而非沉重的义务。

你是否曾经见证过你所爱之人绽放与成长？对我而言，这是我所见证过的最美丽的事物。

□

By 李·西库塔

[image]
[image]

S11关系结构革命-总章节

[image]	关键词	
[image]	创建时间	2025年11月1日 6:00 (GMT+8)
[image]	**Description**	关系结构革命

[image] [image]

[image]

建设中！敬请期待。

[image]
[image]

社区应该是什么，是谁在玩坏这个概念：关系结构革命 S11E02

[image] 关键词	
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2025年11月3日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

解放结构：关系结构革命 S11E03

[image] 关键词	
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2025年11月4日
[image] **Description**	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

如何与内部冲突共存

[image] 关键词	[image]S11关系结构革命-总章节
[image] 关联	2025年11月10日
[image] 创建时间	关系结构革命
[image] **Description**	

[image]

[image]

建设中！敬请期待。

[image]
[image]

如何组织社交空间

[image] 关键词	亲密团队 人际安全 关系 团体 沟通 组织
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2025年11月15日
[image] Description	关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

结识新认识的人时您应该曝光自己多少信息？- 原则和技巧

[image] 关键词	交往 人际安全 分身 协作
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2025年11月17日
[image] Description	关系结构革命

第一印象很重要，安全同样重要。

- Table of Contents

自披露原则1：保持披露内容对称
自我披露原则2：逐步深化会话交流
自公开原则＃3：积极主动地领导
自我披露原则4：平衡问题和评论
自我披露原则5：不要吹嘘，即便您所言完全属实
自我披露原则6：不要让自己显得无所不知
假身份
一些可以帮助您改善身份外观的小建议
1、穿上 适合 您的衣服。
2、照顾基本的卫生和修饰。
3、改善姿势。
4、握手要牢固。
5、说话低声，语速稍微拉低。
6、与对方交谈时要看着对方的眼睛。
7、地位感 绝非 霸道。

[image]

曾经有很多朋友询问过这样的问题：我们如何彼此信任？怎样判断一个初识的人是可信的？

也许这是个错误的提问方式。信任需要分级，就如情报机构的做法 —— 那种依靠撒谎来完成任务的工作，所有人都是谎言精通者，这种情况下判断一个成员是否可信是相当有难度的；于是他们划分了严格的知情等级，不同的人分配不同的权限。

这并非是在赞美间谍的工作方式，而是说，这应该是个原则，关于：信任分级。并没有绝对的信任和不信任，也没有固定不变的等级，一切都是动态的，衡量在每时每刻进行着。

[image]

（关于安全等级划分）激进社区用户请从这里进入：[image]信息最小化原则

那么，如何面对初识者？可以给予多少信任？这就是本文希望解释的问题。

这可能是个棘手的问题。

一方面，研究表明，更多地揭示自己的人比被谨慎的人更容易被对方喜欢。公开个人信息会告诉对方您信任他们，重视他们的观点，且希望与他们更接近。正如我们反复讨论的那样，兴趣是对等的。通过向别人显示您对他们的兴趣，他们更有可能对您感兴趣。

一点保留和超然的态度最初可能会引起好奇，并被视为神秘而诱人。但是最终，您的沉默会被看作是冷漠，缺乏兴趣或想要隐藏自己 —— 无论这是一个不愉快的特征，还是仅仅是您没有什么可展示的事实。

第一印象很重要，您肯定不希望错过未来才能发现是最有价值的合作者。

人们想知道你是谁；他们无法与陌生人建立情感联系。亲密关系会激发兴奋（从几乎所有角度来看都是如此），如果没有化学反应就不可能了。

如果您不能在一定程度上放松警惕，新的相识者和潜在的合作者或恋人，都将被推远或感到无聊，或两者兼而有之。

因此，自我披露是颇具价值的，对于建立人们的兴趣和亲密关系至关重要。

但是，另一方面 …… 您可能已经了解到本站的🔥反渗透/线人&减轻背叛的损失-AntiInfiltration&informant 专题中演示的那些可怕的案例，其中攻击者用诱导的操纵手段以获取您的私密信息，并借此打击您和您的组织。

另一方面，公开太多可能并没有吸引力，并且其本身就令人反感。每个人都熟悉 “过度共享” 一词 …… 那么，如何避免陷阱？

接下来将讨论一些简单的原则来平衡自披露的微妙动态。

[image]

自披露原则1：保持披露内容对称

这是共享个人信息时要牢记的首要原则。披露应对称；您应该以与他人相同的速率和强度来揭示有关您自己的事物。

就如《First Impressions》的作者用脱衣扑克游戏做出的类比：您不想光着身子坐在那里，而其他所有人都穿着衣服。

以下两个原则将帮助您了解如何保持披露对称。

自我披露原则2：逐步深化会话交流

交流专家艾伦·加纳曾经概述过让对话进行并变得更加有意义和重要的四个阶段：

- 陈词滥调。这些社交礼仪虽然意义不大，但却可以促进互动：“嗨，你好吗？” 很高兴认识你。”
- 事实。人们交换基本信息。他们来自哪里，他们的工作是什么等等。正如加纳指出的那样，在这个阶段，“彼此双方都在试图找出是否有足够的分享可以引导出一段值得建立的关系。”
- 意见。一旦人们彼此了解些了，就开始介绍自己对时事、体育、金钱、爱情等常规议题的看法。
- 感觉。加纳说：“感觉与事实和观点不同，因为它们不仅可以描述发生的事以及您如何看待发生的事，还可以传达对发生的事的情感反应。” 仅仅分享事实和观点会使对话相对肤浅而干硬。感情则揭示了您的内心，而这才是真正使人们产生兴趣和关注的东西。

谈论 “感觉” 可能是谈话中最有效的方法，但是您肯定不想跳过前面的部分就直接分享感觉。因为这样做通常会导致暴露一个人缺乏自我意识，并招致 “哇！真是太棒了！” 类似的上堆式回应，也就造成了那种难以持续的对话。

相反，您应该逐步完成每个阶段，从较浅的闲聊到较深的交谈，以此来建立起一个过渡。从轻到重，从平凡到深刻，从中性到来电 ……

您如何知道什么时候该开始，或者另一个人何时准备从一个阶段转到下一个阶段？

掌握这样的动态能够帮助您掌握控制谈话节奏的诀窍：如果您意识到自己正在和一个您不想进一步了解的人谈话，并希望尽快脱离，您可以通过保持浅尝辄止的方式来踩刹车，除了交换事实之外，不要有太多的进展；但是，如果您对这个人很有好感，想和他更加亲近，就可

以稍微加快您的上坡路。

在后一种情况下，当您认为自己已经在其中一个阶段花了足够的时间时，可以披露下一个阶段的一些东西，作为一种试探性动作，看看对方是否做出了类似的回应。

例如，如果您一直在交换事实，就第一个提出意见；如果对方提出意见作为回报，那么您就可以在这个阶段花一些时间了。

不过，如果对方没有做出回应，而是坚持分享事实，那就继续在这个阶段多呆一段时间，然后再送上另一个试探。

自公开原则＃3：积极主动地领导

由于披露才能产生亲密关系，所以很多人可能很想一开始就分享沉重的问题 —— 抑郁症、过去的分手烦恼、虐待史、财务问题等等 —— 以某种方式启动结合过程。

但即使在您第一次进入分享意见和感受时，您最初也应该将这些披露保持在一个更积极的轨道上。

负面情绪是一种社会流行病。您必须建立一个积极的背景和兴趣的支架，然后关系才会准备好承受黑暗负担的重量。

如果在这个支架构成之前您提出沉重的问题，就像把一个保龄球放在蜘蛛网上 …… 尤其是，当您是组织负责人或老成员时，保持积极的精神状态才能为新人带来激励。

自我披露原则4：平衡问题和评论

请记得，您不是被动的。向某人提出更多的问题是表达兴趣、表现魅

力和建立融洽关系的有效方法。

提出很多问题也让您有机会控制对话 —— 这很可能是件好事。如果您对社交很有信心，可以帮助把害羞的人从他们的保护壳中吸引出来，甚至把讨论引向您个人感兴趣的话题（当然，理想的情况是，您应该寻求谈论你们双方都感兴趣的话题）。

但要注意，接二连三地提出问题也会暴露您对自己的私人信息的隐藏。这可能会显得您控制欲太强，让人觉得您有什么要隐瞒的，或者自己没有什么有趣的东西可以分享。

虽然错误地提出太多问题与谈论太多关于自己的问题都可能不是好事，但谈话最好是像排球游戏而不是审问，您也应该允许对方向您提问。

当然，并不是每个人都会这样做，即便有机会。但至少在谈话中加入自己的评论和观察，给对方一个专注的倾听者印象，对拉近关系很有好处。

评估您是否在过多和过少的自我披露之间取得了平衡的一个好方法是，在互动结束时问自己："我对对方的了解和他们对我的了解一样多吗？"

如果答案是否定的，那么您要么是说太多了，没有向对方提出足够的问题，要么是您问了太多的问题，对自己的分享不够。下次重新调整您的自我披露速度，目标是让彼此间形成更加平均的动态。

自我披露原则5：不要吹嘘，即便您所言完全属实

人们总是认为 "地位越高，越具有吸引力"，于是往往喜欢将自己的优势摆在前面。比如 读过哪家常春藤名校、得过什么大奖、去过多少个国家旅行、会多少门外语、在哪个大企业做负责人 ……

这些可能都是真实的自我描述，您的确很有实力。但是需要知道，吹嘘是不会讨喜的，您的优势应该被对方去发现，而不是由您自己来描述。

所以，建议您尝试以更加微妙的方式传达您的自我披露议程。

您可以通过交流具体的议题展现您的知识含量，通过故事来描述异国的文化，甚至通过高端的绅士举止来展现您的身份，逐渐渗透对方对您的了解。

另一种不太巧妙的自我披露方法是，在对事物的描述/解释中添加不必要的细节。比如，对于
“您是否经常出差工作？” 这个问题，回答成这样：“是啊，最近三个月我去过巴厘岛、伦敦、莫斯科和格陵兰岛。我总是被要求与世界各地的公司首席执行官会面。实际上，我上周刚认识***大腕。”

虽然可以提出 “回旋镖问题” 并以一种微妙的方式添加讨人喜欢的细节，但实际上，如果您说得太多了，效果会完全相反。它只能显示您的不安全感，从而降低了您试图证明的身份。

[image]

自我披露原则6：不要让自己显得无所不知

您也许真的非常博学，并且见多识广，也或许您很擅长用主持人的模式控制对话，但是当您与对方不太熟悉的情况下，请注意这点：您不应该让自己看起来无所不知。

您知道我们每个人都有自己最擅长的领域，如果您的最擅长恰好与对话的另一方的擅长具有很高的重合率，理论上这是一件幸事，它意味着你们之间将有更多话题可聊，关系会能够迅速拉近。

但是，这种情况下尤其是要注意，您不应该抢话，而是要努力让对话节奏保持在对等 —— 如果您回答了2个问题，那么下面2个问题就应

该让给对方来回答，您作为提问者，尽管您知道答案是什么。

如果对方滔滔不绝，您也可以在适当的时候插入自己的意见，最好以问题的方式，从而引导对话回归对等的节奏。

即便您是组织领导者，也需要这样做，甚至需要/应该更多地让渡回答权给对方；让对方感觉在您这里获得了被重视的兴奋。每个人都喜欢自己被重视，而您很容易就可以为对方制造这样的感觉，也许您会因此获得一个很积极的合作伙伴。

假身份

如果您必须使用假身份，那就应该从始至终使用同一套完整的假身份。您必需牢记它，切勿前后矛盾，一旦对方产生怀疑，结果很可能对您不利 —— 如果对方原本是恶意的，您的疏忽会打草惊蛇；如果对方非恶意就更麻烦了，您将很难再与对方构建互信。

我们绝对不会建议您使用全套假身份 ，除非您是调查记者，正在卧底。当然，如果是这样，您肯定已经知道该怎么做。

这里需要强调的是分身。在从事敏感的工作中您需要有一套独立的私人身份概况，这个概况不应该与您的任何真实身份重叠 —— 包括兴趣爱好和审美品位、求学经历和工作经历。

也就是说，作为敏感组织的领导人或参与者，您创建假身份目的应该仅仅是为了便于彼此间的对话和合作，而不是瞒骗 —— 这非常重要。

[image]

激进社区用户请从这里进入：[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

以及这里：分身

您的想法、立场、出谋划策的智慧，必须都是完全真诚的；简单说，您在工作/合作中所展示的一切都应该是完全真诚的， 除了 您的名字和家庭背景之外。这就是原则。

遮遮掩掩绝不会帮您构建任何好的合作关系。真正的合作者也不会过度关心您的个人私事，而是关注您的能力和特长如何协调组织工作的顺利进行。在这样的情况下，您的自我介绍应该只是为了帮助构建彼此间的熟悉。

如果有其他人对您的私人信息感兴趣，也不必马上竖起红旗，要知道聊些私事的确是一些人表达亲切感的常用方法，但是您心里应该始终有一个界限：有必要说什么和没必要说什么。当对方的提问触及 “没必要” 的部分时，您随时可以礼貌地转移话题。如上，控制对话的节奏对您来说会很有利。

[image]

不论是急切的还是长线钓鱼模式的，每一个渗透者都会带着明确的目的而来，

如果您发现一个新人带有明显的目的性，而不是自我能力的展示性，您应该小心，

因为这不符合人的心理常态。

在这种情况下您首先应该做的是为其分配低权限的知情等级，就如本文一开始所介绍的，然后继续观察。请注意，要保持谦逊的心态，不要被自己的第一印象所误导，因为您可能随时会发现事情并非如此；万一您的第一印象有误，您的下意识心理排斥所表现出的举止会造成对组织不利的影响。

低知情权限并不意味着看起来不团结。团结协作的融洽气氛并不仅仅展示给您认为可疑的某个人，而是对所有参与者来说都是如此。作为领导者，您应该随时记得这点，这事关您的组织能力。

[image]

一些可以帮助您改善身份外观的小建议

提到“身份”这个词也许人们会首先想到阶层地位，其实这是个误解。身份不仅包含财富，还可以包含其他任何东西 —— 可以为他人提供某种价值的东西。它可以与您的品貌、技能、健康状况、智力、洞察力、创造力、个性特征、社交关系，甚至是查找和共享信息的能力相关联。

简单说，地位和收益的损失不仅体现在一个人的银行账户上，也体现在 —— 人们是否会回应您的笑话、是否赞美您的外表、是否邀请您参加聚会、是否对您表达羡慕、是否向您寻求建议 …… 等等，上千种方式。

在当今世界，有许多不同的群体，每个群体都有自己的价值观和地位标准。但是，还有一系列在时间和文化上几乎普遍享有的标准。培养这些特质，无论您身在何处，无论做什么都可以提高您的地位感，并有助于增加您在社区组织和更广阔世界中的整体影响力。

这些特征构成了地位的基本基础，因此，即使您最终没有在任何一个特定的利基市场中脱颖而出，您仍然会感受到健康、拥有强大的社会支持、以及干练的能力发挥。

毫无疑问，就您自己的自我价值和他人对您的评价而言，您的内在技能和特质应该是最重要的。但是，如果您的外观和肢体语言一开始就没有吸引他们，人们可能永远不会了解这些看不见的特质。

通过增强外观和肢体语言，您可以与人们的基本兴趣点打交道，而不是与它们对抗，从而使人们更容易了解您。这一举动既要自我服务，又要慷慨大方。

目标仅仅是让您的“包装”准确并成功地宣传您的内涵。将您的外表和举止视作为您的内在人提供无缝的展现门户。

其实做起来并不那么难。

1、穿上 适合 您的衣服。

即使您拥有优美的形体，衣服也是非常重要的，并且在人们如何看待您方面起着至关重要的作用。

因此，如果您身体健康，那么可以穿上可以增强身材的视觉效果的衣服；如果身体状况不佳，您需要找到可以淡化弱点并改善整体外观的服饰。

不论是运动外套还是您穿的其他衣服，合体性都是非常重要的。指导原则是，织物应紧贴皮肤而不会挤压或收缩。到处走动时，您不应感到被拉扯，但也不应有任何松动下垂的感觉。西装和衬衫应量身定制，以使其在您的腰部勾勒轮廓，能充分显示您的气质。

如果您超重，但正在努力让自己保持健康，那么健身就显得尤为重要。但是如果穿着合适的衣服，您可以钝化这些不良状态信号。

2、照顾基本的卫生和修饰。

保持基本的容貌和卫生状况可以大大改善您的身体状况。真的，它不仅能给您健康和活力的面貌，而且还能体现您的尽职尽责，这是几乎每个人都珍视的特质。

其实非常简单，只需执行小时候妈妈教给您的东西即可：每天洗澡、刷牙、用牙线清洁、淡雅体香，并保持面部毛发整齐。头皮屑、粉刺等问题虽然看起来不起眼，但都会在整体上影响您的身份表达。需要注意并妥善处理。

3、改善姿势。

中文里面有个词语“仪态”，这个词出现的地方往往很传统和教条，它与某些礼仪密切相关。但我们这里谈到的姿态与此不同，它不仅仅关乎礼仪，更关于您的自我表达。

您的肢体语言在传达您的地位方面起了很大作用。

如果一个人认为自己的地位很低，就通常会采取一种顺从的姿势，例如弓背或低头。如果您看起来很低落，其他人就会认为您很低落。

因此，请抬起下巴挺直背部（不要抬得太高，否则会显得自大）。

[image]

4、握手要牢固。

握手是体现身份的另种形式，坚定的握手与主导地位和自信有关。软弱的握手充满顺从和不确定性。

如果您想传达身份地位感，就需要有力地、大方地、充满自信地握手。但是，请不要抓得过牢。

下面这些您应该避免……

5、说话低声，语速稍微拉低。

说话音调较低的人被认为比说话音调较高的人具有更高的涵养。一项研究发现，阶层和语调之间存在相关性，声音越低，地位越高。

实际上研究人员发现，音调降低25%就能使地位感明显抬升。大自然决定了您是否拥有优美的嗓音，但您可以做一些简单的事来加深和改

善声音的魅力。

有修养的人说话也比较慢，并且不会担心沉默。如果说话速度很快、急于填补任何安静的时刻，都会让您显得紧张和缺乏安全感。

其实很容易改善这点，只需要做到仅在您有话要说的时候才讲话。

6、与对方交谈时要看着对方的眼睛。

研究表明，频繁地进行眼神交流的人们被认为具有更高的自信和实力、更高的地位和风度。不自信的人会下意识地减少眼神交流，通常会最先避免注视。

对于社交焦虑症来说，这可能是具有挑战性的，但是通过实践，您很快就会能克服恐惧。

请确保正确的、平等感的、体贴的眼神交流，绝不是审判式的，不是死盯着对方，更不是挑逗。这也许听起来很微妙，您或许觉得难以控制？其实并不难，您无需控制眼睛，只要调整自己的心态到正确的位置，眼神就会自然表达出成熟稳重的魅力。

7、地位感 绝非 霸道。

霸气的方式真的有可能令您在短时间内获得统治地位，但是，从长远看来，您肯定会失去同龄人的尊重。没有人喜欢被欺负，您也绝对不会期待自己的队友表现出臣服。

拥有能够帮助社会群体的才能和技能的人才能获得长期的尊重和地位，最重要的是，愿意为同龄人的利益分享这些才能和技能。慷慨才能构建稳固的身份。

5-羟色胺使人感到镇定、社交欲望和控制感。血清素水平随着人的一

种状态而增加，并随着另一种状态而下降。因此，经常遭遇身份失败的人血清素水平可能很低，这会导致敌对行为，而敌对和攻击性只会令一个人的地位低下保持更长的时间。这是一个自欺欺人的循环。

但是这一循环是完全可以被打破的。研究表明，可以通过训练自己，将注意力转移到自己和同等地位的人身上，并开始专注于如何让自己对他人有用。

好了，基本就是这样。希望能帮到您。记得多练习！

[image]
[image]

在这个操蛋的世界里，奋力地相爱！—— 情人节2026

[image] 关键词	亲密关系 关系 反叛 爱 结构革命 自助 训练
[image] 关联	[image]S11关系结构革命-总章节；[image]S10战友爱侣 - 总章节: 爱，关系，嫉妒，拒绝和解放
[image] 创建时间	2026年2月14日
[image] **Description**	关系结构革命

中文有老话说，“成大事者，先过情关”。这话在一定程度上是有道理的。你知道为什么吗？

世上没有天然“对的人”。但你完全可以通过恰当的心理技巧，将每一段关系培育成“对的”样子。怎么做？

传统“核心家庭”是维持支配性等级压迫体制的关键基础设施。任何不能彻底拆除这一基础设施的“革命”都不会带来解放，只是 而已。

以基于平等和自主的关系取代等级制度和核心家庭，是重要的反抗政治实践；但这需要反抗者经历一场艰辛的修行。别担心，这是有技巧的。

- Table of Contents

  引言
  如果你也有经历过以下情况，这本书就是为你写的：
  1. 主流文化脚本仍在塑造我们的“关系”
  嗨宝，你正在读一本自助手册。你可能会想：

身处困境倍感煎熬
打破陈旧的文化脚本
我并没有说这一切都是你的心理作用
浪漫神话：关于爱的谎言
浪漫神话的核心谎言
爱的转化力量？
浪漫神话如何搞砸了我们彼此间的关系？
区分冲突和虐待
关于爱的真相
婚姻并不等于爱、更跟“解放”没有任何关系
浪漫神话如何侵蚀情感关系自助工具
匮乏心态
用后即弃的文化
“其他事实是什么？”被文化脚本和自动反应束缚时如何获得新视角
“其他事实是什么？” 工作表
请填写下面表格：
现在，请就以下问题做些笔记：
为什么要费力做这些情绪修行？这能给我带来什么？
人真的能改变吗？
“宽容VS.严谨” 评估工具
关于浪漫关系（或他们所谓的“婚姻”）自助手册的一些注记
惯习成就自我
第一章小结
2. 困于自驾模式：在麻木与短暂的亢奋间摇摆
在痛苦的世界里靠麻木维生
整体麻木，却在追逐幻象
培养对微妙和细致的觉知
重拾完整的情感谱系
培养情感觉知的工具
情感范围受限的代价
麻木与情感劳动
麻木和体面政治
麻木和微歧视
关于麻木与追逐幻象的问卷
责任担当：既不淡化，也不惩罚
反馈问卷
追逐关于性和浪漫的文化幻象
这是强迫行为、成瘾倾向，还是正常现象？
请勿贴标签、不要评判 —— 不要将本书的观点“武器化”

“上头”的感觉
沉迷于“新关系能量”？
这种追逐的后果

[image] 家，就是爱的样子。

本书致力于提供的是一份实用的路线图，教你如何应对最常见的关系冲突模式，以及在情绪高涨时管理本能反应的有效工具。这本书能帮你建立你所渴望的、具有支持力的解放性的关系，并巩固你所珍视的团队社群和抵抗运动。

一份关于性事、爱恋、浪漫和友谊的自助指南。献给天下所有爱侣和战士们！

[image]

引言

> 这世间一切值得做的事，都是与他人共同完成的。
> —— 玛丽安·卡巴，《就这样做下去直到我们获得自由》（We Do This ’Til We Free Us）

> 提升感知与被感知的能力—— 即“喜悦”—— 意味着更加贴近这个正在流血、燃烧和尖叫的世界……“自由”并非没有约束，也不是随心所欲的个人主义，而是一种在关系中耕耘、转化欲望、并打破固有习性的新兴能力。
> —— 卡拉·伯格曼和尼克·蒙哥马利《快乐的抵抗》（Joyful Militancy）

二十年来，我一直投身于社会运动，致力于终结刑事化和暴力，去构建一个所有人都能各取所需的社会。在跨性别解放、反战、以及废除监狱运动中，我曾担任律师、作家和组织者。参与这些抵抗运动是我一生中最大的快乐之源，也是我获得诸多深厚友谊的基石。虽然当下的生存环境极其残酷，但我从研究抗争、参与抵抗运动，以及与那些为解放事业奉献终生的人们并肩作战的过程中，汲取到了丰富的灵感

和力量。

然而，抗争运动本身也是激烈冲突的爆发地 —— 冲突固然存在于我们与权力阶层之间，但也同样频繁发生于运动内部。革命的能量营造了一种在政治和个人层面上都高度紧绷的氛围。由于运动中既涉及“我们该共同做什么”的路线之争，又掺杂了性格差异，这些冲突常常成为工作的阻碍。

组织者之间产生友谊乃至性关系，都并不奇怪。在激情燃烧的地方，共同的价值观和目标毫无疑问会带来强烈的归属感和亲密感。我们理所当然会和运动中那些性感、聪慧之人 —— 那些理解我们的思想并愿意为解放志业而战的人 —— 走到一起。作为一名女权主义者和酷儿，我深知性作为转化、表达和社群构建的场域有多么的重要。性关系和浪漫关系令人心潮澎湃，它们是自我发现、彼此支持和互相治愈的重要载体。事实上，许多人加入抵抗运动就是为了寻找志同道合的人。可以说，性和其他形式的联结与抗争工作总是如影随形的 —— 我们在运动中找到了渴望已久的关系，不言自明。

但这种炽热联结带来的兴奋感，并不能保证关系会一帆风顺。在运动中与他人日复一日地合作，我屡屡目睹并亲历组织者之间关系冲突的杀伤力。即使是那些毕生恪守原则的人，在亲密关系中也可能做出违背原则的事，而且往往是下意识的。

为什么我们有勇气大胆挑战主流社会的规范和结构，却常常难以用体贴和慷慨来对待身边的伴侣？为什么一旦陷入不安、失望或嫉妒，我们就丢掉了原则？为什么我们在性与浪漫关系中总是表现出最糟糕的一面？又是为什么，我们会将浪漫关系置于友谊等其他关系之上？

我一次次地看到，在关系中将价值观转化为行动是多么的困难。我亲眼目睹了人们在对待伴侣时的行为如何导致团队瓦解、项目流产，甚至摧毁了我们的事业。我也曾深刻反思过自己的行为，运用了无数工具方法以寻求改变，并帮助我的指导对象和合作者转化他们身上这些具有破坏性的模式。

我写这本书，是因为代价真的太高了：我相信，我们可以、也必须将最激进、最具有远见的解放理念融入到我们的性、爱、浪漫实践，以

及生命中所有的“关系”中来。我们现在比以往任何时候都更需要彼此，我们必须学会如何紧紧凝聚在一起，哪怕在情绪失控的时刻。

这本书并不提供速效药或“30天包治百病”的仙丹配方，现实生活中并不存在那种东西。本书致力于提供的是一份实用的路线图，教你如何应对最常见的关系冲突模式，以及在情绪高涨时管理本能反应的有效工具。这本书能帮你建立你所渴望的、具有支持力的解放性的关系，并巩固你所珍视的团体队伍和抵抗运动。

为了将原则更充分地融入关系之中，我们需要：

1. 理解那些定义了“理想关系”的文化信息和守旧观念。

1. 识别这些预设和文化“脚本”是如何影响我们自身的行为和反应的。

1. 采取实际步骤来平复那些本能的或“被操纵”的反应，使行为回归到我们对待自己和他人的初衷。

在本书中，我将分享来自我个人生活以及我参与的运动中合作伙伴们的故事。这些故事关乎我们许多人都曾深陷其中的各种关系乱麻。我还将提供一些思考题和练习，帮你深入挖掘那些有害的文化叙事是如何影响你对关系的期待和沟通的。这些练习是摆脱文化奴役的第一步。

[image]

著名的女权主义口号“个人即政治”是正确的：亲密关系中的点滴至关重要。

浪漫生活不仅仅关乎个人的成败。在性、爱恋和浪漫的问题上，我们每个人都承受着文化规范的压力，也都需要支持来“卸载”那些病态的思想和行为。

通过性、浪漫、爱和友谊，我们可以培养关于解放与欢愉的新体验。

我们都渴望被真正“看见”、被关爱，渴望联结感与炙热的恋情，渴望体验快乐和创造力。

而为了实现这一切，我们需要将关于自由与正义的深刻思考，与对疗愈和联结的渴望，

密切结合起来。

[image]

[image]

返回：

返回：

返回：

返回：

我之前的著作看起来可能与这本书大相径庭。我的第一本书《常态生活》（*Normal Life*）探讨了弱势群体如何承受福利制度、移民政策、警务和医疗改革带来的冲击，并探索了抗争运动（尤其是跨性别解放运动）如何避免被收编或被挫败。第二本书《互助》（*Mutual Aid*）研究了我们如何通过互助组织有效协作，以应对当下的（以及未来的）危机，而不是乞求政府或企业的施舍。对我而言，这第三本书是我的核心研究课题的延续，关于：我们如何才能建立起持久且有效的抵抗运动？阻碍运动的屏障是什么？我们如何克服这些障碍？并且，本书为这个研究项目增加了一个极具人情味的维度 —— 一份关于性事、爱恋、浪漫和友谊的自助指南。

主流的情感自助类畅销书能带来的启发非常有限。虽然有些书对特定行为模式有不错的洞察，但它们几乎都保留了过时的、往往带有性别

歧视色彩的性爱观念。而且很少有作品不以白人、异性恋、上流社会的生活为中心，这极大地限制了它们的参考价值，尤其是对那些身处抵抗运动中的人们来说。

大多数此类书籍是由治疗师基于个人经验或伴侣咨询案例撰写而成的，或者是某些自诩为万人迷或沟通高手的人写出的。而我是一名律师、教授和活动家，了解我的约会史的人都不会说我是什么情感高手。但我是一名长期的运动参与者和观察者，二十五年来我一直在不懈地努力改进我的各种关系。

关于如何对待彼此，我所读到过的最深刻的见解并非来自心理医生，而是来自奥德雷·洛德、贝尔·胡克斯、劳伦·贝兰特、小山惠美、希拉·哈桑、马里亚梅·卡巴等作者。这些人对“关系”问题的洞察力和智慧源于他们身处危机社群和正义运动的实践经验。这并非巧合。

[image]

这本书是写给那些有动力通过每段关系的尝试一次次一遍遍地集体抵抗规范性文化预期的读者们的，也正是关于他们的故事。

为了做到这一点，我们必须向内看，去“卸载”那些我们自幼被灌输的文化烙印。

谈到性、爱恋和友谊，最具破坏性的文化叙事 —— 即我在书中称之为“脚本”的东西 —— 当属“浪漫神话”。这种神话告诉人们，浪漫关系是生命中“最重要的关系”，是每个人获得完整、满足、被爱、和安全感的“终极归属”。

美国和加拿大的调查显示，现在人们将“爱情”列为人生第一目标，甚至排在金钱成功和职业成就之上。而在20世纪30年代，爱仅排在第五位，排在可靠的品格、情绪成熟和讨喜的性格之后。现在，人们比以往任何时候都更期待在浪漫伴侣那里满足所有的亲密和安全需求。在电影、广告和电视剧的影响下，浪漫的“爱”已经成了满足所有情感、性及陪伴需求的万灵丹。这种将浪漫爱置于至高无上地位的观念，促使人们在爱情来临时忽视友谊，并催生了在性与浪漫中的不安感、紧迫感和竞争意识。

浪漫神话告诉人们，浪漫是永恒的且排他的，被爱（或去爱）意味着“属于”（或“拥有”）某人。它宣称，如果你有不同的需求或欲望，那一定是你自己、你的爱、或你的伴侣出了问题，因为“真爱”应该是轻松的、自然的且永恒不变的。

当我把这些话说得如此直白时，想必很多人能看出这些信息是多么不切实际且具有伤害性。在这种神话的影响下，浪漫之爱往往遵循一个可预见的周期：从令人沉醉的狂热开始，随后进入充满失望和怨恨的冲突期。你可以看到这种“占有和拥有”的模式是如何导致伤害和控制行为的。简而言之，我们看着朋友们 —— 以及我们自己 —— 因为对浪漫关系的幻觉而做出糟糕的决定、毁掉生活、互相伤害。

然而，我们大多数人仍被这种浪漫神话所困扰。当约会不顺时，我们会把它看作“个人”的失败。我们认定是自己的错，觉得自己选错了人，觉得只要下次选个“更好的”，就能打破循环。我们在社群里评判和指责前任，对他们冷嘲热讽；或是因为缺乏某种特定形式的浪漫关系而严苛地评判自己，无视生命中友谊和其他情感纽带的重要性。这正是“文化脚本”在扭曲我们的期望和行为的案例之一，正是它从根本上破坏了我们建立满意的、激励人心的且符合伦理的关系的能力。

[image]

这本书激励人们做出决定：浪漫并非独立于我们的解放斗争和抵抗政治之外。

关系是践行我们的原则和价值观的 实验场 ，

而不是排演企业媒体喂给我们的那些烂剧本的舞台。

如果我们想建设一个基于关怀、联结和自由的世界，就必须将在“外部”所做的工作、与在“亲密生活”中严谨的自我修持，结合起来。

我们现在太需要彼此了。

在这个操蛋的世界里，我们必须学会如何为了爱和抗争而走到一起。

如果你也有经历过以下情况，这本书就是为你写的：

- 总是在重复同一种分手模式。
- 沉迷于交友软件，但又因选择匮乏而感到疲惫、厌倦和挫败。
- 因友情或爱情的动荡导致朋友圈子四分五裂 —— 朋友们会因为新恋情而消失，或者在分手事件中站队，导致群体分裂。
- 在恋爱关系中感到孤立，渴望拥有更多的亲密朋友。
- 曾遭受某人的伤害，如今正督促所有其他人与那人绝交，所到之处摧枯拉朽一片狼藉。
- 苦苦渴求完美的爱恋、理想的工作、或完美的身材，认为那能“解决一切问题”。
- 一直试图做到完美，当收到批评建议时会感到沮丧或本能地防御；或者因为太害怕负面评价而不敢尝试新事物。
- 无法停止照顾身边的每个人，不知道该如何拒绝他人，感到既委屈又疲惫。
- 不知道该如何接纳友谊、浪漫约会或其他关系，即便内心欢喜，却还是不断地把人往外推。
- 经常觉得“我讨厌人类”。抽象地相信同理心、联结和集体行动，但防御性地厌倦他人。
- 对活动家团体中不断出现的冲突感到疲惫不堪，尽管你也很想/

> 仍然很想要参与集体变革，却对加入新的行动或团体的前景感到绝望。

不管你是不是“异议人士”或者活动家、不论你是否激进，生活在资本主义世界中的大多数人至少经历过上述问题的一种，很可能是多种。希望这本书能帮到你。

[image] 是啊，的确如此。 [image]

1. 主流文化脚本仍在塑造我们的“关系”

> 我并不是说清醒地活在这个世界上不痛苦。但请保持清醒，亲爱的。
> —— 玛莎·P·约翰逊

> 我用爱人的指尖
> 勾勒你下颌的曲线
> 深知最艰巨的战斗
> 仅仅是开端
> 该如何带着尊严与爱
> 去完成生存之必需
> 我们选择了彼此
> 也选择了彼此战斗的锋芒
> 这场战争始终如一……
> —— 奥德雷·洛德（Audre Lorde）

主流文化用海量的图像轰炸人们，将浪漫爱标榜为“幸福的关键”。许多人拥有或渴望拥有惊心动魄的性与浪漫体验，希望以此为生活带来兴奋、愉悦，以及一种被珍视、被接纳的强大感。与此同时，我们大多数人也注意到，人们往往在面对爱人时表现得最糟糕，且常为了追求浪漫联结而牺牲掉了其他关系和优先事项。更糟的是，人们被灌输了一种观念：关系中不可避免出现的问题，都是因为你自己或朋友、爱人、伴侣的“缺点”造成的；人们很少想到，关系中的困扰其实源于并且服务于那些强大的统治与控制体系。在浪漫关系中（无论是酷儿

还是异性恋），亲密伴侣暴力发生率高达 30%，更有无数段关系滋生着让人们感到孤立、恐惧、乏味、不被爱、焦虑或被困的情感动态。

[image]
[image]

甚至在 COVID-19 疫情之前，996长工时、辛苦的通勤、为了工作学业背井离乡以及沉迷网络，就已经加剧了各阶层的孤立感。疫情以来，这种孤立只是变本加厉，随之而来的还有飞涨的物价和房租、深陷的债务、以及日益加剧的不平等。独自生活的人越来越多，拥有亲密关系的人越来越少。这些因素与“浪漫神话”结合，营造出一种错觉：让人误以为浪漫伴侣“能够且应当”满足我们所有的情感需求。我们被教导着要去寻找一个伴侣，来填满由这些病态现状凿出的深渊。

当然，没有任何人能够或应当满足另一个人的所有需求。通常情况下，当关系陷入困境，我们并没有强大的支持体系来获得见解和帮助。而许多单身的人则陷入了对在线交友的无效痴迷中，在软件上耗费大把的时间，寻求幻想中的满足感，有时还怀揣着不切实际的期待。

我们都见过身边朋友被浪漫伴侣所伤害；见过彼此因为新恋情或感情纠葛而退出深爱的团体和活动；见过朋友圈、活动家集体、职场和艺术合作因性事和浪漫相关的冲突而分崩离析。我们也曾切身感受到被困在艰难关系动态中的痛苦。

当如此多人被困在这些充满压力、消解斗志、使人丧失行动能力的处境中时，我们该如何聚在一起去推翻那些正在伤害大众并摧毁地球的主流体系？…… 为了打破心碎、嫉妒、占有欲、麻木、冲突、孤立和背叛的循环，我们需要理解那些经常左右我们行为与欲望的宏观社会动力。

关于浪漫和性的主流观念延续了统治体系，强化了“关系应该是什么样、感觉应该是什么样”的刻板印象。它们教导我们“应该”去渴求什么；它们告诉我们，某些特质 —— 比如苗条的身材、丰厚的财产或者结婚证书 —— “才能带来”幸福圆满。这些信念，即使我们在理智上明白它们是扭曲的，依然会冲击我们的情感和行为。它们如何侵蚀了我们共同繁荣的能力？我们又该如何摆脱它们的控制？

[image]

识别文化脚本如何影响人的消费欲望相对容易。你的朋友圈子或亚文化圈可能会鼓励你远离油耗高的汽车、血钻或者血汗工厂制造的衣服。

然而，强大的文化脚本往往也决定了我们在性事与浪漫方面的需求。

我们被教导关系“应该是”排他的、是长久的，而且还会遵循“预设的”升级模式。

但就像有毒的商品一样，这些社会预设的准则同样具有破坏性。

当我们误将这些文化脚本的灌输当作自己的感受和愿望时，

我们的“关系”就会遵循 主流文化为我们设定的伤害性模式 。

我们常将嫉妒、孤独、痴迷等强烈情绪视为自然的、不可避免的或不可抗拒的。我们甚至可能意识不到自己正受控于性和浪漫的神话，只因这些感受如此私密，就仿佛源自每个人的内心。但种子其实是主流文化信息播下的。

我们必须“卸载”这种制约，才能 找到更具支持性和转化性的方式来，渴望彼此、相伴彼此。

本章内容将仔细审视一些塑造了我们在关系中的感受和行为的文化脚本。理解这些文化烙印如何塑造情感，以及其带来的困境，这就是我们挣脱束缚的起点。我们将深入探讨几项练习，练习如何察觉并开始摆脱控制，从而建立我们真正想要且需要的联结。

[image]

嗨宝，你正在读一本自助手册。你可能会想：

- 我没时间看这个。
- 我害怕审视自己的感受。
- 如果我深挖自己的过去，我可能就没法“正常”生活了。
- 我害怕改变生活中的任何事。
- 直言顾虑会让我被甩吧？
- 我需要隐藏，我害怕真实的自我没人会喜欢。
- 这些东西很俗气/玄学。
- 这是弱者才会看的东西。
- 这类个人主义的“自助”鬼话都是自由派和中产阶级玩弄的东西，只会分散集体行动的注意力。
- ……

这些是许多人在考虑接受治疗、阅读自助手册或做其他可能触及情绪、行为模式和反应的事情时经常产生的情绪。你可以觉察到这些情绪，然后继续读下去。你可以问问自己，这些想法是从哪儿来的——你脑海里响起的究竟是谁的声音？是你想追随的人的声音吗？你可以提醒自己，阅读这本书不会导致任何事情失控 —— 你依然可以选择如何处理读到的内容。你可以提醒自己最初拿起这本书的原因：你的生活中是否有某些想要改变的事情，与你在关系中的感受或反应有关？你是否能意识到，提升处理关系的能力可帮你更有效地参与抵抗运动？当消极念头浮现时，记住你的初衷会有所帮助。你也可以制定一个支持计划：有没有朋友可以跟你交流这本书的内容？能否读慢一点？在阅读时能否做些让自己放松的事？没必要急着读完，也没必要

非得用学到的东西去做什么。保持好奇心就足够。

[image]

身处困境倍感煎熬

我们生活在一个高压时代。虽然技术让人类看起来比以往任何时候都更自由、联系更紧密，但每天我们都要面对激增的不平等、恐怖的生态危机和无休止的战争。我们中许多人已经受够了，渴望改变，并共同努力反击。但与此同时，感觉就像我们只是在网上吵架，而现实世界的一切都在变得更糟。许多人感到无力，甚至难以想象一个不被贪婪、等级制和剥削定义的社会。与此同时，我们被淹没在各种屏幕分心和麻木自我的新方式中，这加剧了我们与他人及自然世界的脱节。为了应对，我们被迫消费那些能带来短期快感（或假性快感）的东西，但这往往导致身心的长期失衡，并加剧我们的孤立。

[image]

人类在群体中进化，通过共享一切来生存。

我们天生就需要联结和交往。关心彼此并努力让事情变得更好，会让我们的生活充满意义、满足感、创造力、喜悦和归属感。

拥有亲密关系和可以依靠的人，决定了我们在危机中是否安全，甚至决定了我们能否生存。

而我们身处的这个社会系统告诉每个人说，除非你有钱、有型儿、有精英的工作、坐拥各种名牌物品、或者必须结个婚，才会“幸福”。

这个社会训练我们将彼此视为可弃置的“东西”，让我们在等级森严的体系中衡量自己，从而产生自我否定感。

我们与周围人的关系构成了我们的世界；人和关系就是世界。

我们需要 解放这些关系 。

人类是社会性动物：我们需要彼此。我们无法独自生存，无论我们是否承认这种相互依恋，它都决定了我们生活的一切。关于“独立个体”的文化幻想掩盖了我们对他人的本质依赖，贬低并忽视了支撑我们生活的照护活动（打扫、烹饪、扶老携幼、情感支撑）。种族资本主义——这种助长少数人掠夺财富、多数人遭受苦难的全球种族剥削体系 —— 教导人们将自己视为“个体”，为了私利而相互竞争。

[image]

只要能打破“独立”的幻觉，就会发现我们已经存在于一个生存所必需的互助网络之中 —— 我们所需的一切都来自彼此和这个星球。只是这个网络一直在被暴力和胁迫所扭曲，以便让少数人获利。

我们的任务是抵抗并摧毁那些将我们的生命转化为剥削性和破坏地球产业之燃料的体系。

我们必须 开辟崭新的共生之道 、 同时也要 重拾古老的生存智慧 ，那些能够滋养生命、联结、归属感和解放精神的生存之道。

然而，从我们出生那天起，这些技能就不断被文化脚本所破坏和阻挠。我们被教导要去竞争、要追求个人主义、要保持贪婪、要遵从/誓死捍卫森严的等级。

- 倘若我们遭遇冲突时不必执着于谁对谁错呢？
- 如果我们将冲突视为任何关系中可预见且具有建设性的一部分呢？
- 如果我们都能从朋友那里获得足够的支持，从而足够抵御冲突或分手的风暴呢？
- 如果我们平时就非常擅长给予和接受反馈，以至于我们的关系不会频繁堕入怨恨或在戏剧性的结局中爆发呢？

考虑到我们所处的世界环境，感到恐惧和不知所措是正常的。而关键问题在于：在这些艰难时期，我们该如何相互扶持，采取勇敢大胆的行动，并变得更善于在这一切中彼此相爱？如果我们想共同渡过难关，就必须摆脱那些关于爱与关系的狭隘制约。

[image]

- 你见过哪些因素导致朋友圈子或社群中发生冲突和疏离？

- 你能否想象，或者你是否经历过，人际关系中的差异和冲突反而带来了更多的联结、归属感、自主性和创造力，而非削弱这些特质？是什么支撑着这种现象？

[image] [image] 无产阶级的故事

打破陈旧的文化脚本

想要获得 解放 ， 就需要有看清事物真相的能力 。

主流文化的脚本 —— 性别歧视、种族主义、资本主义和殖民主义 —— 如同棱镜折射光线一样扭曲每个人的认知，让我们对自己和周围的人产生偏差的愿景。

[image]

“文化脚本”通过无休止的重复植入人们的内心；

随后，你就会以“自动驾驶”的模式度过一生，

在没有自觉思考的情况下演练这些脚本。

这种“自动驾驶”意味着，我们的许多回应、行为、甚至感受，其实并不真正属于我们。它们是被程序化植入的，而我们自己在不知不觉中机械型性地重复它们。

当某人处于自动驾驶状态中时，就不会质疑自己的假设或本能的反应；也意识不到自己的行为往往背离了原则。自动驾驶的一个后果是，它经常会导致人们陷入两极化的思维 —— 导致人们失去了细致和复杂性，思考方式变得极端，比如："我是最烂的！"、"我做不到！"、"都是她的错！"、"这永远都行不通！"、"怎么总特么发生这种事！"……

在本书中，我们将使用钟摆（如下图所示）的意象，来探讨当我们处于反应性思维或恐惧状态中时，那些极端的、往往两极化的想法是如何产生的。目标是与这种反应性思维保持足够的批判性距离，从而在情绪激动时打破它对我们的控制。

下面的钟摆图探讨了一种常见的反应性两极化思维：认为自己是"最好的"、或是"最坏的"。这两者可能都不是事实，但当一个人被激怒时，就很容易滑向其中一端。

[image]

钟摆示意图说明：

- 一端：我是最好的！（自大、防御、拒绝反馈、指责他人）

- 另一端：我是最坏的！（羞愧、自我厌恶、瘫痪感、受害者心态）

- 中间：我既不是最好的，也不是最坏的。（人性化的、细致的、有责任感的、愿意学习的）

因为我们所有人都生活在一个推崇归咎、惩罚和等级制度的社会里，大多数人遭遇冲突时会在这两极之间摇摆。当陷入"我是最烂的"思维时，如果能察觉到某种异常 —— 即我们对现实的认知已然扭曲 —— 或许就能意识到需要寻求帮助、或寻找新的视角。如果没能察觉，就可能伤害自己或他人。比如，可能开始认定自己永远是受害者，从而认为自己"有权"发泄情绪，或者无视他人对自身行为影响的反馈。讽刺的是，自认"最差劲"的羞耻感反而会导致无法倾听亲近之人的心声，无力回应他们的诉求 —— 因为这种情况下此人会始终陷在自我

贬低的思维漩涡中。如果能察觉到"我最差劲"的念头何时浮现于脑海，就能挣脱其控制，不再遵循其预设的脚本。

“我是最好的！”这种感觉可能很不错。但它会导致你错误地假设别人是错的，或者误以为自己知道什么对别人“最好”。

在这两种情况下都不存在任何认真的倾听。可能变得封闭僵化油盐不进、固执己见，从而破坏了与他人的联结。

当我们发现自己处于这些极端情绪中、无法感知局势的细微差别时，通常属于一种恐惧驱动的条件反射状态，这种状态会在关系中产生严重的冲突和伤害。

[image]

在处理情绪激烈的局面时，请牢记这句话：“我既不是最好的，也不是最坏的”，可有助于找到反证，反驳那些最偏激的自我叙事，从而转向更稳健的行动基础。

识别那些阻碍解放的习性，可以帮助我们在被扭曲认知控制时建立警觉。

通过探讨一些常见的被内化的文化脚本，我们可以更有意识地选择在关系中的行为。

我并没有说这一切都是你的心理作用

自助手册这种东西最糟糕的一点就是，它们很可能让人误以为：无论“我”遇到什么问题，只要改变自己、自己的思维、自己的态度，一切就都会变好起来。这绝对是胡扯。我们都生活在恶劣的现实环境中，摆脱恶劣的唯一出路是摧毁种族资本主义、父权制和殖民主义的集体行动。但与此同时，这些东西确实钻进了每个人的脑袋。我们被胁迫着去执行它的设计，成为可能虐待、统治和囚禁他人的人。我们被洗脑，对自身或他人的屈服心安理得。因此，我们需要同时进行内在的修持和外在的反抗。

健全主义、年龄歧视、种族主义、性别规范强制和肥胖羞辱，在制造孤立方面都起到了巨大作用。它们导致人们贬低彼此，并将特定的身体描绘成“不讨喜的”。我深刻意识到这些规范如何决定了许多人获得性、爱、陪伴和友谊的机会。我们必须共同转变我们的朋友圈子、社交圈子和亚文化圈层，推翻这些残酷的“讨喜度”等级制度。

[image] “鉴于近日一位网络名人的死亡引起的关于厌食症等心理健康问题的话题”

浪漫神话：关于爱的谎言

浪漫并非与生俱来的天性；它是一系列通过反复强化以形成的、服务于支配体系的文化规范和期待。歌词、电视剧、电影以及来自家庭、朋友和社群的信息都在告诉人们，浪漫爱是生活的中心，是幸福的关键。然而，在历史上，浪漫爱并不总是组建家庭甚至都不是选择性伴侣的基础 —— 它有一段被发明被部署的历史，就像其他被描绘成“自然”和“普世”的有害结构那样（如白人至上和天命论）。

浪漫的概念具有文化特异性，并非一直存在，且随时间而改变。历史上大多数人类都通过社群关怀来组织生活，照顾病患和抚养孩子，这些往往都在婚姻或一夫一妻制的框架之外。在不同的时代和地域，性的表达有着极其多样的形式。即使在我居住的美国这种工业消费社会里，研究也表明，过去人们对通过浪漫关系满足需求的期待远低于当下。

[image]

随着我们每个人面临着日益严重的孤立、友谊的缩减、以及社群内部支持的消失，我们被迫依赖一段浪漫关系来提供每一种我们需要的关怀。

[image]

当前的主流模式 —— 核心家庭 —— 是为了取代从事自主农业的大家庭族群而出现的。

随着资本主义需要更多流动性的工业和服务业工资劳动者，浪漫爱成

为了将人们困在体系中的社会结构之一，而这个体系旨在榨取劳动者和整个地球生态，只为让极少数人变得富有。

现在的税收、财产、医疗、住房和移民体系都是围绕“婚姻家庭单元”设计的。无论我们是否以此组织生活，这个规范都是当下的蓝图。

我们被告知它是“自然的”，但实际上它只是目前占据主导地位的一种特定设计。

从这个意义上说人们关于性和浪漫的想法只是种族资本主义的产物，尽管其感觉非常私人。

解放我们的“关系”的过程，需要我们意识到这些欲望并非发自内心，并且，尤其是，我们完全可以选择去培养和追求什么。

[image]

浪漫神话的核心谎言

你一定听过下面这些BS：

- “一段稳定的浪漫关系/性关系是所有关系中最重要的。”
- “如果你没有处在一段关系中，那你肯定是有问题、有病、说明了你是没人要的丑陋的废柴。”
- “真正的爱永恒不灭。”
- “找到对的人/正确的关系就会让你获得幸福。”
- ……

浪漫神话告诉你，这世界上有一个“真命天子/天女”在等着你。它宣称，如果你能找到并留住那个人，曼妙的性和爱就能自然、持久、且轻松地永续。这种神话坚称你“不会再”被其他任何人吸引，且你们会始终如一地感受到彼此的爱意与性魅力。它还教导浪漫伴侣从关系伊始就该遵循一系列递进的台阶：达成性排他的“主义级”的协议、搬到一起住、许下终身承诺、财务合并、以及生儿育女。如果有人不想要这些，那此人一定“有问题”；或者TA压根“不是真爱”，再或者TA只是太自私。浪漫神话宣称，如果你的爱是真的，你就能够且应当为了对方而放弃一切。

浪漫神话还教导我们要去竞争“尽可能最好的”伴侣。请注意，所谓“最好”是由种族、经济、社会性别、健康和身材标准来定义的。约会变成了一个竞争市场；因此，你要确保为自己的长期承诺找到一个尽可能“优秀”的配偶，并在可能的时候以性为交易“向上攀爬” ……我们都被要求去恐惧孤独、恐惧被抛弃、恐惧被一个“卢瑟（失败者）”伴侣所拖累。于是，我们透过一种算计的、评估的、竞争的眼光审视彼此，每个人都根据植根于压迫性规范的标准来争夺“最好”的伴侣。这导致了人的“非人化” —— 我们将彼此像商品一样评估，而某些人则被贴上“不受欢迎”的标签。

爱的转化力量？

这本书对浪漫和爱的态度如此尖锐，你可能会问：那爱的转化力量呢？生活在一个被浪漫神话催眠的社会里，我们不断听到关于“浪漫爱可以使人更完整”的夸大承诺，所以我不会在这里聚焦于此。然而，我确实认为，性与浪漫关系 —— 正因为它们能激起人们如此强烈的反应 —— 完全可以是深入了解我们彼此的内心创伤和文化制约、并体验治愈性联结的深刻场所。

我姐姐曾告诉我，焦糖是厨房里最危险的东西，因为它可以烧得滚烫，非常容易造成严重烫伤。性与浪漫的关系亦然，它们极度甜美，但也充满风险。然许多冒险的事都是值得的：离开虐待你的家庭或宗教社群、保护朋友不被警察抓走、阻拦运煤火车和石油管道、占屋居住、接管校园、打破规则、创作艺术 …… 等等。

[image]

本书支持冒险，支持性，支持各种形式的爱，

但它也要求你我直面我们在性与浪漫关系中的行为如何经常伤害自己、伤害他人，以及如何因此影响了我们的社会运动。

我希望书中的内容能帮你找到方法，去获得所有你想要的、解放的愉悦。

我希望我们每个人都能感受到那种来自团结的爱，来自对弱者的关怀、来自与朋友或陌生人并肩采取大胆行动、来自与充满生机的地球相联结、以及来自共同打破枷锁的 —— 爱。

[image]

浪漫神话如何搞砸了我们彼此间的关系？

由于浪漫神话暗示每个人“都应该”遵循同样的预设步骤来获得爱和满足，它导致人们对他人的需求和渴望产生了一种想当然的推测；它让你假设伴侣的性、社交、或其他需求都是“正常的” —— 要么和你自己的偏好一样，要么和你从主流文化脚本中解读出来的所谓“正常态”一致。它导致人们产生负面的自我审判或相互审判，一旦某人不想要那些所谓的“正常” —— 例如，有人想要成年后一直独居，或者性需求比“应该有的”更少或更多，或者完全不渴望婚姻 …… 就注定遭到审判。

这些浪漫神话导致许多人在根本没有充分思考的情况下就做出了重大的人生决定，比如为了伴侣的工作搬到远方，抛下朋友和社群；它导致我们对友谊和其他支持圈投入不足，将爱人置于朋友之上，这往往导致孤立；浪漫神话要求我们以爱的名义“放弃”一部分自我，这常使我们在应对生活挑战（包括浪漫关系内部的挑战）时缺乏准备或支持。浪漫神话还将嫉妒和占有欲合理化，这会激化冲突，甚至被用来为虐待开脱。

在浪漫神话的影响下，怨恨滋生，人们陷入停滞不前的互相指责的动力之中。“如果你真的爱我，你就肯定会 ……”：

- “在我想要的时候跟我做爱”
- “跟我结婚”
- “搬到一起住”
- “跟我生个孩子”
- “放弃某项我不赞成的活动”
- “把更多的时间花在我身上，而不是和朋友在一起或独处”
- “戒除你的那个习惯/行为因为我不喜欢”
- “接受我的某种行为/习惯，即使你因此受到伤害”
- “花时间陪我的家人，即使他们虐待你/甚或咱俩一块被虐”

这些在关系中浮现的浪漫神话观念可能出现在普通的冲突中；但也可能是一系列虐待模式的一部分。建立一种意识以识别“这些观念如何进入我的大脑并塑造期望”，将有助于理清我们自己真正的需求。不过仅仅如此还无法解决虐待模式。

区分冲突和虐待

对于“冲突”与“虐待”的区别，并没有单一完美的定义，但反暴力运动的智者们长期坚称：虐待关系包含一个人试图通过重复的模式对另一人维持的控制，并拒绝为造成的伤害承担责任。我们偶尔都会产生控制他人的冲动，也会有时对他人造成伤害。但虐待发生于一种更持久的权力不对等、控制和虐待的模式中。不论任何时候，如果有人正在实施或遭受虐待，这种局势需要比处理非虐待性冲突更坚定的边界和更多的支持。

区分冲突和虐待并不容易，且代价巨大。正如专门从事冲突调解的引导师威亚姆·哈德比安所说：“人们试图通过将某事定性为‘冲突’来淡化虐待，又通过将‘冲突’定性为虐待来夸大问题。” 另一位冲突引导专家乔维达·罗斯观察到：“将虐待当作冲突处理是为更多虐待做铺垫，而将冲突误判为虐待本身也可能是一种施加控制的手段。”

本书无法彻底解决这个挑战，但希望能提供工具，有助于更好地理解我们自己的经历及其对他人的影响，并建立基于同意的关系。如果你正试图弄清楚自己的关系是否属于虐待，向外寻求支持至关重要：你可以找朋友聊聊，寻求治疗师的帮助，或拨打热线电话。

关于爱的真相

[image]

真相是，没有任何“一个”人能满足你“所有”的情感需求。

拥有更多种类的联结会让我们更安全、处境更好；

当我们与许多人建立信任和联结时，就更容易在生存和抗争中保持创造力和耐力。

世上并不存在所谓的“正常”生存方式或交往方式。

如果你想让别人理解你的渴望、希望自己被如何对待，你就必须直接告诉他们。

不要猜心。

对方完全可以对你的要求说“是”或“不”；

如果他们说“不”，你可以寻求在别处满足需求，

或者自我满足，

或者在需求未被满足的情况下继续生活。

尽管主流文化发出了强烈的信号，但并没有什么“绝对正常”的方式去体验浪漫或性。即使是持久、有趣、双向且非常愉悦的性关系，也需要不断的协商与重新协商，并且肯定会经历潮起潮落。变化是不可避免的，改变并不是背叛。同样，尽管面临一夫一妻制规范的沉重压力，真相是：被伴侣之外的人吸引（甚至是强烈的吸引）并不意味着你们的关系有问题。

与此同时，对新人的强烈吸引并不意味着你别无选择只能去追求对方，也不意味着他们就是你的“宿命”。新的吸引力不能成为欺骗的借口。稳定的伴侣关系、多边恋情关系、炮友关系、一夫一妻制关系、一夜情和匿名性行为、短期关系、以及所谓的“开放式关系”，在政治和道德上都是完全平等的。性或浪漫联结的形式并没有优劣之分、并没有哪个比哪个“更进步”。关于关系类型的价值等级制度通常会阻碍人们的自我决定，并延续羞耻、背叛、欺骗、疏离和不满的模式。

真相是，并没有任何一段关系会自动让你幸福。进入每一段关系时你都会带着自己长期的情感模式和设定。关系虽然“换了”，但你依然是那个你。浪漫和性关系可以成为了解自我和成长的场所，特别是，因为它们能激起强烈的、复杂的情绪，并经常触动一个人的童年或原生家庭的创伤。但它们并不比其他关系更必要或更重要。

新恋情带来的美好感受不仅源于对方，更源于我们自身建立联结、感受喜悦、体验愉悦、激发创造力与感受兴奋的能力。我们能够也应当将这些能力融入到各种关系与活动中，而不仅限于浪漫关系。

尽管浪漫神话执着于“白头偕老”，但维持关系还是选择分手，本身并无好坏之分。两者都是成长的契机。试图占有对方或控制对方、或者试图控制任何人的思想和情绪，都是徒劳且痛苦的。委屈自己、压抑欲望会产生无尽的怨恨和蔑视。理想的关系应该支持一个人的全面发展，培育一个人的渴望，而不是将其视为威胁。

浪漫神话告诉人们伴侣是“稀缺的”，或者“更好的”就在转角处，或者每个人一生中“只有一个对的人”。这种“匮乏思维”服务于消费文化 —— 它不断让人感到自惭形秽，也可能让人觉得别无选择只能留在事实上已经无法维持的关系中。这都是假象。

我们生活在一个充满无限社交可能性的世界，虽然种族主义、肥胖羞辱、厌女症、性别二元论、阶级歧视、年龄歧视、地域、语言和残障歧视等等，确实影响着性和约会的范围，但“匮乏框架”并不能帮助我们共同抵御这些压迫。与浪漫关系相关的需求 —— 如性满足、肢体亲密、被肯定、共享欢愉、彼此陪伴、共进晚餐和同居 —— 都可以通过友谊、家人和/或与自我的关系来满足。事实上，我稍后会讨论，加入抗争团体虽然并不总是轻松，却是寻找同道中人的绝佳方式。

[image]

婚姻并不等于爱、更跟“解放”没有任何关系

从定义上讲，女权主义、黑人解放和酷儿解放等反主流文化的运动质疑着主流文化，也包括主流文化中关于美丑、渴望、或禁忌的所有脚本，以及关于人们“应该如何”交往和组建家庭的脚本。

在 60、70 和 80 年代，女权主义者和酷儿打破了关于家庭暴力和儿童性虐待的沉默，揭露了婚姻作为一种社会控制形式、以及“核心”家庭作为针对妇女儿童暴力场所的真面目。当时的反抗者致力于简化离婚程序，并挑战那些污名化非婚生子女的法律结构；他们揭穿并反驳了那些将黑人社区的贫困状况归咎于“低结婚率”的种族主义观点。在这些运动中，年轻人创造了颂扬随性性行为、公共性行为、非生殖性行为、同性性行为、单亲抚养、非婚同居、替代性家庭结构、BDSM（特殊性癖好）、纯友谊关系、互助关怀社群、以及女性性愉悦的亚文化。这些努力的核心是对婚姻的批判 —— 婚姻被视为控制女性的手段、积累财富的工具，更是一个奖励顺从政府家庭规范的系统。

然而，在 80年代，这些解放思想遭到了反扑。主流系统收编了女权主义和酷儿的符号与概念，抽空了它们的激进潜力，并将一个无牙的空洞的版本假扮成“解放”重新兜售给人们。

在 90 年代和 2000 年代，由白人律师领导的一批非营利组织开展了同性婚姻倡导，将婚姻描绘成“爱与联结的场所”，尽管毫无疑问，婚姻显然/且永远都是国家进行社会控制的一种工具性结构。由此婚姻被重新定义为酷儿想要“加入”的东西，而不是从根本上需要“摧毁”的东西。酷儿不再是浪漫神话的威胁，而是突然被赋予了这种特定的强制力，还被裹上了“自由”的幌子。

[image]

人与人的交往方式牵动着 巨大的利益 —— 体制深知这一点，

体制总是想要干预我们的关系，

孤立我们，

挥霍我们的时间，

耗尽我们的精力，

挑拨我们彼此互相对立。

努力抵抗这种顺从的压力，让我们与几代反抗者联系在一起，

他们曾为 拆除核心家庭规范、建立革命性的共处方式 ，奋斗终生。

[image]

• 浪漫神话的哪些部分让你感到熟悉？有哪些部分依然束缚着你？你能想到浪漫神话曾如何阻碍了你的浪漫关系吗？具体说说？
• “关于爱的真相” 这一节中，有哪些观点读起来让你感到刺耳？有哪些让你感到解脱？
• 在浪漫神话的影响下，你是否曾做出过违背真实性格或价值观的行为？在你了解到这一切背后的操纵性之后，现在的你会怎么做？

[image]

浪漫神话如何侵蚀情感关系自助工具

那些标榜“能带来洞察力”的约会与关系自助手册，往往与主流的浪漫神话“同流合污” —— 过度抬高传统的浪漫伴侣关系，同时贬低其他类型的关系。

自助手册经常争辩说，浪漫关系“天然”至关重要。依恋理论畅销书《抱紧我》（*Hold Me Tight*）的作者苏·约翰逊博士写道：“爱是 …… 进化的巅峰，是人类物种最引人注目的生存机制 …… 因为它驱动我们与少数珍贵的他人建立情感纽带，为我们提供避风港。” 而事实上，每个人当下的孤立状态（许多人根本没有或很少有亲密关系）是种族资本主义和殖民主义创造出来的社会条件的产物。将其归结为“人类进化”而非“社会控制”，既失实又误导。

约翰逊和许多人一样，引用了“已婚人士寿命更长” 这类根本上有问题的统计数据。情感孤立确实是健康风险，但以此宣称婚姻关系是“最健康、最进化的生活组织方式”，纯属无稽之谈。例如，普遍存在的家庭暴力现实该如何解释呢？

宣称人类在生物学上“天生”倾向于某些特定的关系、并因此认为这些关系“更优越”，是极其危险的。在约翰逊的作品以及许多所谓的“关系自助手册”中，都包含了类似的有害论调：声称“稳定的长期关系永远优于随性的性行为”。

匮乏心态

从孩提时代起，你我就被教导着要为联结的渴望而与他人展开竞争 —— 竞争最好的成绩、“有面子”的工作、“拿得出手”的约会对象等等。我们的心态在“比较和绝望”中恶性循环，总在试图搞清楚自己比别人好还是差。我们被告知，如果搞砸了跌到等级制度的最底层，就会流落街头、被抛弃、甚至死掉。我们被训练成总是“向上看”，盯着别人有而我们没有的东西，同时忽视那些处境不如我们的人的经历。在大多数生活领域，即使并没有面临真实的匮乏，人们也一直遭受着

恐惧和“匮乏感”的驱动。

当你处于匮乏心态的影响之下时，“匮乏”看起来不像幻觉，而像真实存在的 —— 就像真的没有足够的资源分给每个人，不抢就没了。文化规范就是这样伪装成真理的。匮乏心态阻断了人们的创造力和慷慨，导致人们变得多疑，有时甚至变得不可信。你会觉得永远没有足够的时间、爱、金钱或权力。它千方百计地给你植入恐惧：它告诉你，你很快就会老得没人要啦，或者你必须“升级”你的身材、你的人脉资源、你的社会地位、房子或车子的档次。而事实上，所有这些东西 —— 获得更多的关注、财产或地位 —— 都不会让你幸福。

[image]

研究幸福感的心理学家讨论过“内在动机”与“外在动机”的区别。

“内在动机”指的是：你做这件事是因为你珍视它本身；

“外在动机”则是指：你做这件事是为了从外界获得某些东西 —— 好成绩、更多粉丝、晋升或认可。研究发现，实现外在或物质目标（如财务或物质占有）的人并不会变得更幸福。

然而，实现内在目标的人，比如成为一个更细心的朋友、慈爱的父母，或者单纯为了快乐而跳舞、创作艺术，确实会变得显著幸福。

研究显示，一个人的外在动机越强，就越容易感到抑郁和焦虑 —— 关系变得更短暂，质量也随之下降。

这并不奇怪。如果主要是根据地位或财富来评判一个人，就不太可能建立基于相互支持的、温暖且信任的联结。

“富人更幸福”的想法不断被灌输给公众，伴随而来的还有“只要努力，人人都能致富”的成功学神话。在美国，35% 的人相信自己有一天会进入收入最高的前 1%，78% 的美国人认为努力就能致富，尽管财富显然日益集中：富人越来越富，其他人所有人都越来越穷。

[image]

在这些错觉的驱使下，人们不断剥削彼此、剥削环境，在讨厌的工作中苦干，或者花时间试图在社交媒体上成名。

我们学会了竞争而非联结或协作。

种族资本主义鼓励人们 认同精英 ， 以至于 投票支持精英的利益（哪怕损害自身利益），

因为人们错误地相信自己“总有一天”会成为那些精英。

不会的，永远都不会 —— 为了生存，站起来反抗那 1% 才是至关重要的。

研究显示，消费商业媒体（看电视和上网）都会导致变得更追求物质。那些花大量时间思考想买什么的人，同理心和慷慨度都会降低，最终将他人视为物品。物质主义对我们的关系和福祉都非常有害。

研究人员发现，你拥有的亲密朋友数量比收入、传统美貌、智力或教育程度更能预测幸福感。然而，很多人却以牺牲亲密关系为代价去竞拼攀爬。广告通过在人们心中植入不安感和焦虑来促进消费，我们每天暴露在 4,000 到 10,000 条广告中。认出麦当劳标志的18个月大婴儿比认识自己姓氏的还多。平均而言，到孩子36个月大时，就已经能认识100个品牌标志了。

对我们大多数人来说，这种物质主义和地位导向影响了我们的约会和性观念。我们不断复制着广告商灌输的且被社交媒体上无限放大的“人际吸引力等级制度”。我们沦为了攀附者，根据地位排名来衡量自己和约会对象，而这些排名通常与财富、苗条、健康、种族和性别规范挂钩。甚至在性、爱、和浪漫的领域，我们也变成了浅薄、自恨的消费者。

物质主义对“完美”的强调 —— 竞争谁看起来更幸福、展示更完美的

生活 —— 还强调思考方式的”正能量“，同时羞辱“负面”情绪。事实上真正让生活有意义的是拥有亲密联结的关系，成为所关心的事业的一部分，帮助他人，并在阻止不公中发挥作用。这些任务需要建立（或重建）深刻感受痛苦的能力：共同的愤怒，共同的恐惧。陷入匮乏心态时，就很难聚在一起互相照顾，更不用说共同反击了。

当前的局势已经非常操蛋且严峻，我们需要共患难的技能，正如我们需要共享乐的技能一样。我们只是试图让生活在社交媒体照片中看起来很美 —— 充满地位象征物、和令人艳羡的经历 —— 这阻碍了去创建和维系我们所渴望的关系。正是这些关系 —— 而非别人对我们的看法 —— 才能支撑我们度过艰难的时刻。

[image]

- 你是如何体验匮乏心态的？
- 物质主义在哪些方面阻碍了你的幸福？
- 你是否有过摆脱匮乏思维的经历？
- 你在什么时候会享受内在价值带来的快乐？

[image] [image] [image]

用后即弃的文化

从童年起，我们就听闻世上有两种人：“好人”和“坏人”。这让我们终其一生都在恐惧被贴上“坏人”的标签，并拼命争取被视为“好人”。我们很早就学会隐藏一部分自我以换取“好人”的标签。许多这类教诲是非言语的，由照顾者通过行为示范，界定什么是可接受的边界。

作为孩子，我们极其脆弱，察觉什么能获得认可、联结和安全感，是生存的本能。我们也从大众媒体、身边同龄人以及自己或他人因越界而遭受的羞辱中学习。例如通过压抑愤怒或假装对“女孩子气”的东西感兴趣来学习做一个“乖女孩”；或者内化了各种规模的禁忌 —— 闭上嘴巴咀嚼、不在公共场合穿得太露、保持优雅不许哭、不许大叫、去抱抱亲戚不管你喜不喜欢那个人、对着镜头笑…

这些教诲在早期就根深蒂固了，并跟随我们进入成年。弃置文化在每个人心中植入了恐惧：只要做错一件事，你就会被驱逐。如果我说错

了话，会失去朋友吗？如果别人知道我真实的样子，我会遭到排斥吗？…… 人们变得害怕给予和接受反馈，变得极具防御性；同时学会千方百计给他人挑刺儿，以突显我们自己的优越。潜意识里明白，暴露他人的缺陷可以让“我”赢得尊重、并保护自己的社会地位。

然而，其结果 —— 背后中伤、社交媒体网暴、以及“墙倒众人推” —— 会伤及所有个人并撕裂团体。在理想情况下，每个人都应该能够给予和接受批评性的反馈，以便从错误中成长并改善关系。但由于受到弃置文化的塑造，很多人一直对批评保持警惕，确保自己不会是下一个被扔掉的人。矛盾的是，身处弃置文化创造的高风险环境中，还可能导致我们隐瞒所爱之人的伤害行为，因为担心他们会被严酷审判。尤其在浪漫关系中，人们经常选择向朋友隐瞒自己的约会对象所犯下的伤害行为，因为怕朋友觉得那个对象是“坏人”。随着孤立感增加，处境会变得更加危险。

现实中，刻板的弃置规范并不符合我们的生活。我们都可能还爱着某个曾伤害过我们或他人的家人；或可能有个关系极好的朋友，尽管他喝醉后很糟糕、或者在金钱上不可靠。我们从生活经验中知道人是复杂的，伤害行为往往源于创伤，但生活在弃置文化中让我们很难记住这一点。

[image]

为什么会生活在弃置文化中？——

我们生活的这个世界是建立在“将某些人视为非人”的基础上的。

为了证明殖民主义和奴隶制的正当性，一些意识形态被创造出来，使整个人群变得“可以”被剥削、“可以”被杀戮。

要维持这种排他性的社会工程，并说服所有人“将数百万人（主要是原住民、黑人和棕色人种）关进笼子是合理的”，就需要一整套弃置意识形态。

它需要一种 叙事 ：为了保护和培养那些被视为“好的”、“值得的”、和“正常的”人，可以随意践踏另一部分人性。

在个人层面上，我们中许多人在两极间摆动。有时担心自己被看作“坏人”：「我说错话了吗？大家会不会发现我是个装逼犯，根本没资格待在这儿？」有时会沉溺于自己的道德优越感。很少花足够时间待在细致的中间地带，即认识到：每个人都在学习、犯错、冒险和尝试。当冲突引发强烈情绪时，我们往往进入激烈的 “好人/坏人” 模式，将爱人、朋友、家人和同事变成扁平化的反面教材。

当人们互相伤害时，通常默认采取两种极端立场之一：要么淡化伤害，要么惩罚伤害者。这个社会一直在淡化种族主义和性别歧视等有害体系的影响，告诉人们对歧视和性骚扰要“看开点”、脸皮厚点、别生气。假装某些伤害是“正常”或“必要的”，甚至根本不是伤害，比如刑事系统宣称对被捕者进行脱衣搜身不是一种性暴力。另方面，有些人因违反规则或仅仅被指控，就面临巨大的惩罚 —— 逮捕、驱逐、监禁、失去孩子、工作和住房。下面的钟摆图代表了这种“惩罚”与“淡化伤害”的极端。

[image]

当你默认这两种极端时，就会错过中间的东西 ——问责。问责是指评估影响、并制定尺度适中的回应。承认有人受了伤；思考为什么会发生这种情况，如何防止再次发生，以及如何尝试修复。

问责发生于当我们坦诚且慈悲地审视伤害发生的原因，并旨在使其停止的时候。

伤害实施者（以及可能实施类似伤害的所有人）需要什么才能不再重犯？情感支持？关于性、性别和关系的更准确的信息？酒精滥用方面的支持？安全的住房？受害者（以及处境相似的人）需要什么才能感到更安全？稳定的上下班接送、特定夜晚的托儿服务、更安全的住处、理解和安慰？…… 问责意味着我们审视并处理所有让伤害成为可能的条件，而不是否认其发生或寻找替罪羊。

[image] 2024年上映的恐怖电影“The Substance”。女主角丽萨恐惧的并不是“衰老”这一自然现象，而是因衰老而被抛弃、被鄙视、被嘲弄、终生的努力和成就被一笔勾销的羞辱。 [image]

- 你是否曾担心自己被视为“坏人”而被某个团体踢出去？

- 你是否曾经经历过痛苦或伤害，却遭到他人的轻描淡写无动于衷？

- 你是否参与过背后嚼舌头 - 对他人的污名化或排斥？

- 害怕自己被拉帮结派的小圈子排挤，会如何影响你的行为？

- 你是否经历过“不打不相识”的故事？ - 冲突反而让人们学会如何更好地对待彼此、并形成更牢固纽带的例子；

- “承诺不抛弃任何人”这件事，让你感到恐惧的地方在哪里？

- 面对伤害，你认为人们应该如何判断什么是“尺度适中”的回应？

[image]

“其他事实是什么？”被文化脚本和自动反应束缚时如何获得新视角

有时，当你陷入扭曲的、二元对立的想法和感受中时 —— 纠结于自己有多糟糕，或者别人有多糟糕，或者觉得只要某件事发生/不发生就是”世界末日“ —— 你需要获得一些新的视角。

一个非常简单的工具就是问问自己：“其他事实是什么？” 这个问题能帮你发现，偏激的反应是如何让自己的思维变窄的。

例如，如果我嫉妒自己的伴侣，过度关注他们的新约会对象的迷人之处，并对我们的关系感到不安，我可以问问自己：“其他事实是什么？” —— 我可以列一张清单，写下我和伴侣之间的关系进展良好的迹象；写下我选择非一夫一妻制的原因；写下我成功度过的其他困境；写下为什么我认为伴侣不会仅仅因为与另一个爱人建立联结就离开我。

下文将提供“其他事实是什么？”工作表，在你对性、浪漫关系和约会经历产生强烈反应时，它会非常有用。它也适用于工作、家庭、创意合作、活动家团体和朋友之间的问题。你可以独自填写，也可以请朋友协作 —— 如果他们能帮你看到你自己不容易觉察的部分那就太好了。

“其他事实是什么？”工作表

我正强烈感受到的事：____________（例如：小新把我排除在项目之外了，我恨他；或者“这个圈子”表现出的性别歧视和那些垃圾言语，真是烂透了。）

[image]

1、在上图中的小圆圈里写下你正强烈感受到的事。 在大圆圈的其他部分，写下关于这个人/团体的其他真实情况 —— 列出他们的优点、益处或任何能显示出更全面图景的其他事实经历。（例如：“小新去年在项目中是一个非常支持我的合作伙伴，我看到了他的细致、并跟他学到了很多”；“当其他圈子歧视排挤某人时这个圈子曾经站出来维护正义”；“这个圈子在某些方面的确很努力地践行其使命”…）

[image]

2、在小圆圈里写下你正强烈感受到的事。 在大圆圈的其他部分，记录下你“不了解”的、可能正在促成这一局面的情况；“对于对方的意图，我有什么是不确定的？”（例如：“也许小新在做这个决定时并没有针对我，只是对项目本身的权衡”；“也许小新正受到某种个人危机的冲击，导致了他现在的行为”；“也许这个圈子中的某些人也不支持那些歧视性的言语，他们只是没有机会表达反驳”……）

[image]

3、在小圆圈里写下你正强烈感受到的事。 在大圆圈的其他部分，写下除了这件事之外，你目前的生活中还有哪些真实存在的状况？你还在处理其他什么事？你还拥有谁的支持？谁为你挺身而出？谁喜欢你？（例如：“我跟小佩以及大牛有紧密且有意义的合作”；“我最好的朋友让我感到被爱和被看见”；“最近正在读的书让我感到兴奋”；“我有朋友和我一样认为反歧视永远不应妥协”；“过去和未来很多年的经验经历让我意识到目前这件事只是一个小瞬间”……）

请填写下面表格：

我的责任是什么？我能控制或贡献什么？

[image]

哪些东西事实上超出了我的责任和控制范围

[image]

顺便说，有些人喜欢把右边的表格撕掉，或者象征性地烧掉它。

现在，请就以下问题做些笔记：

- 这段经历是否触碰到了我过往经历中的某些痛处？
- 当下的处境是否唤醒了我某种熟悉的角色模式？哪些感受似曾相识？
- 在这种情绪被激活的时候，我该如何善待那些伤痛或过往历史？（勾选以下所有适用项，可在下方无限补充你自己喜欢的方式。）

  □ 吃一顿小时候最爱吃的饭 —— 那段童年时光正与现在的感受呼应。

  □ 多睡午觉，以应对这种压力带来的消耗。

  □ 请一位愿意理解我的朋友倾听我讲述这些感受。

  □ 走进大自然，允许自己为过往类似的遭遇哀悼。

  □ 泡个热水澡。

□ 早点上床睡觉。

□ 请一天假。

□ 活动身体。

□ 写下涌现出的任何情绪。

□ 你的方式是什么？写下来。

为什么要费力做这些情绪修行？这能给我带来什么？

二十出头刚开始接受心理咨询时，我曾担心如果去探索关于母亲病世的哀恸，我的生活会分崩离析。从十二岁母亲病倒起，我就一直压抑着悲伤和孤独。压抑这些情感曾帮我度过了难关：一边应付学业，一边在青春期的社交中周旋，同时还要照顾母亲，随后又经历她去世的打击，搬进寄养家庭。

但拒绝感受这些情绪是有沉重代价的。由于压抑了记忆，我的整体记忆力一度变得很差；由于压抑了感受，我变得冷漠，且很容易被激惹，对情感认知普遍封闭。

我对自己的行为和感受对他人的影响缺乏责任感。我形成了一套焦虑和压力的应对机制，把深层的恐惧牢牢禁锢起来了。我开始接受心理咨询是因为这些应对机制导致了人际关系的混乱和痛苦，但我当时极度恐惧：担心一旦释放被压抑的悲怆我整个人就会垮掉。

而事实证明，探索那些感受并没有淹没我。相反，由于我在性格形成期练习的是如何“压抑”而非“沉溺”，那些情感只是逐渐变得清晰可感。

现在，经过几十年的情绪修行，当我能够触及那份哀恸、孤独或愤怒，去回忆对母亲的思念以及发生过的一切时，我感到了一种解脱。尽管这些感受往往转瞬即逝、难以捕捉，但我还是想分享这一点，因为我希望当年那个不敢推开情感之门的自己能知道：情绪洪水并不会摧毁生活和应对能力。相反，触摸这些感受让我更能抵达真实的自我，建立与他人的联结，并践行我的人生初衷。 我不再被迫缩在那个作为一个恐惧的孩子为了自保而发明的小盒子里。

[image]

我们生活在一套试图 扭曲 我们的欲望的体系中，

这些被扭曲的欲望被利用来维持统治结构的稳固。

我们被要求将非凡的联结与关怀能力局限在“浪漫神话”的狭小范围内。

我们不被鼓励去发现彼此、去建立能转化自我的深层关系，去摧毁种族资本主义，去实现集体疗愈并创造解放的共处方式。

这本书的观点是关于改变我们与自己、与他人之间的关系，从而获得全新的激情、愤怒、愉悦和力量。

当松开文化制约的枷锁、选择符合自身信念的相处方式时，我们就会能体验到：

- 摆脱毒性关系和扭曲的互动模式。
- 感到更有活力、更多好奇心和创造力，从让人瘫痪的绝望中复苏。
- 提升为了追求目标而冒险的能力，以及对不确定性的耐受力。
- 建立强大的友谊和互助网络，体验到被许多人理解见证和支持

的欣慰，同时也成为他人的后盾。

- 享受性、约会和浪漫带来的愉悦，而不会因此毁掉生活。
- 增强对自己和他人的信任感，拥有更多的安全感。
- 避免职业倦怠或从中恢复，学会如何以一种令人振奋而非耗竭的方式与他人协作。
- 能够体验哀伤、难过和愤怒，而不是通过“断连”来逃避，或因压抑这些情感而受苦。
- 能够对不想要的事物大大方方说“不”，根据价值观和目标在人际、机构和活动中设立健康边界。
- 能够学习新事物、实验、试错、倾听反馈、并再次尝试。
- 感受到自己属于地球，欣然承担守护这个星球的使命，为自己和他人的生存而奋斗。

[image]

获得自由意味着自我“去程序化”，

意味着要去洞察那些不被鼓励洞察的真相，去感受那些不被鼓励感受的情感。

我们正致力于在程序化反应之外，恢复更广泛的应对世界的能力。

- 虽然社会教导我在职场或家庭的日常屈辱中感到羞耻和自我厌恶，但我仍然可以恢复感到愤怒、悲痛、并以此激发行动的能力；

- 虽然我被程序设定为试图支配他人，但我仍然可以选择扩展协作和谦逊的能力……

我们可以摆脱那些因重复而形成的惯性反应，

以更符合我们真实信念和目标的方式去回应情境和他人。

这种疗愈的意义在于提升我们去感受和实践新事物的能力，让我们的生活更具有目标感。

这与追求“变得快乐”不同。在主流资本主义文化和流行自助手册中，“快乐”有着相对狭隘且刻板的定义。这种想象中的快乐被认为意味着“一直感觉良好”，而这通常源于实现了某种规范性的成功指标，如结婚、富有、拥有房产和理想的身材。与之并存的信念是：任何“坏”感受——愤怒、恐惧、哀恸、困惑、心碎——都是“需要被治疗的病症”。

这种通过变美、变富、结婚而获得的平庸且安抚式的“快乐”幻象，是消费文化的命脉，它与我们真正渴求的那种充满活力的、敏锐响应的、深层联结的能力完全不同。关于快乐的教条（认为它来自外部、它可以永久实现）很可能只会导致你更不快乐。无论人们获得多少金钱或权力，总会想要更多。永无止境。当人们终于得到心心念念的阶级地位象征物时，往往会发现它完全令人失望。

[image]

与其寻求“快乐”，本书更关乎如何面向现实觉醒，摆脱幻象和习性。

这意味着我们需要允许自己去感受生活在这个充满剥削、战争和生态破坏的世界所产生的恐惧和哀伤。

这意味着我们必须学会独立于“浪漫神话”去与人联结，通过驱散被灌输的“弃置”和“匮乏”观念，更清晰地看待彼此。

当我们决定以基于现实的方式与彼此及自我共处时，

才能以符合价值观的方式去回应这个危机中的世界。

[image]

人真的能改变吗？

通过实践这类自助手册中介绍的方法，究竟能改变多少？

医疗专家、制药公司、通俗心理学家和伪科学来源都在告诉人们：某些根深蒂固的反应是“终生不可更改的”。有些人也觉得自己无法改变，因为创伤经历已经从根本上重设或限制了他们的情感模式和行为范围。

另方面，营销世界又宣称能在“短短30天内!!!”让人脱胎换骨。有些人热切地尝试一个又一个自我改造计划和方法，每次都期待着激进的蜕变……

那么，在“彻底停滞”和“彻底重生”这两个极端之间，究竟存在着怎样的中间地带？

[image]

疗愈/情绪修行的工作 —— 即了解自己的感受、信念，并让行动与价值观一致 —— 是接纳和蜕变的结合，它不是线性发展的。通过使用本书中的工具，我对自己“自动驾驶”式反应、情感范围的局限，以及困境中表现出的僵化或过激，有了更深的觉察。

有时我也会感到挫败，尽管我已然洞悉自己的情感和交往模式，却发现自己还是会做出同样的烂事。我们可能花几十年时间试图改变自己在浪漫关系中的反应和行为 —— 读自助手册、向长辈请教、接受心理咨询 —— 但在艰难时刻，旧习仍会悄然浮现。

可能很难期望仅通过情感疗愈就彻底变成另一个人。那些成长环境留下的创口、为了生存而开发的应激反应，依然会存在。但通过这种疗愈，我们可以降低敏感度，缩短或减少情绪被刺激（变得彻底抓狂）的时间，并开始学习控制伤害性的冲动避免体现在行为上。

[image]

有人说，情感修行是一个螺旋楼梯。

人在向上走的过程中被改变，但也会在绕圈时反复遇到旧伤。

我们做这些修行，是为了下次撞上旧模式的痛苦时，至少能以一种全新的、更慈悲的方式去体验它，并对随后的行动做出新的选择。

个人的蜕变之旅与改变任何习惯是一样的 —— 都需要大量的主动练习以抑制“自动驾驶”模式的行为。有时旧习复发，就会导致偏离轨道。理想情况下，我们可以对自己保持关怀和慈悲，理解蜕变是循序渐进的过程，理解我们曾经依赖旧的应对机制是有正当理由的，即便现在很想要并正在追求新的生活方式，持有这些旧机制也并不代表我们是坏人。通过练习，新习惯会逐渐化为本能，在大多数时候随取随用。虽然不是瞬间完成，但改变是可能的。

[image]

被文化脚本灌输的“匮乏”和“弃置”思维会导致完美主义，即认为某人能够或应该满足社会所有不切实际且有害的理想。

“解放”的过程就应该包括识别并丢弃所有好莱坞、组织化宗教或社交媒体朋友圈动态所描绘的各种不真实的形象。

我们要不断提醒自己和彼此：不要拿你的内心和别人的外表做比较。

我们对他人的真实经历知之甚少，我们的目标是活在自己的生命中、审视自己想做的事和感受、追求对自身有意义的蜕变。

有时我们需要对自己宽容些；有时则需要更多的严谨和主动。

请值得信赖的朋友评估你是否在某一方面走过了头，会很有帮助。

警惕完美主义的危害并培养接纳之心，是挣脱主流体系桎梏的关键所在。

摆脱那些自出生起就被植入我们体内的期待、反应模式、及人际关系模式，绝非易事 —— 即便我们已然察觉到这些模式正在破坏当下的人际关系。我们必须以温柔和慈悲对待自己，体谅自己在充满竞争的、冷漠无情且被抛弃排斥的威胁如影随形的社会中为生存所付出的艰辛努力。在浪漫神话、匮乏心态和弃置文化下生活，恢复的过程是漫长的。但请记得，我们并不孤单。与朋友和合作伙伴谈谈关于交往方式的初衷及其背后的解放原则，能让我们在疗愈中成为彼此的盟友。

[image]

• 你希望改变哪些曾经的人际交往方式？
• 哪些改变看起来更切合实际？
• 过去你是如何促成改变的？
• 你对转变的期望是过高还是过低？
• 在审视自己的情感反应和人际关系时，是什么让你觉得这种“不适感”是值得的？
• 有哪些是你已经能想象到并想要拥有更多的？你能从中学到什么？

[image] [image]

“宽容VS.严谨” 评估工具

在羞耻和自我审判的驱动下，许多人可能会在恰恰需要“宽容”的地方，误以为需要更多的“严谨”——更多的投入、努力、严苛的分析和苦干。同样，如果你一直忽视休息、放松或性生活需求，那可能就需要投入更多精力和专注（即严谨），为生活创造更多容纳这些事务的空间。还有许多领域，由于物质障碍（比如为了付房租不得不干着糟糕的工作），改变是很困难的。而这种探究的目的是寻找在哪些地方增加“宽容”或“严谨”能帮助我们更好的向目标迈进，同时也清醒地认识到，生活中有很多条件是我们无法控制的。

—— 针对以下生活领域考虑这些问题 ——

- 金钱（如：支付账单、根据自身价值观和资源进行消费、在金钱问题上对他人保持诚实）
- 友谊（如：关怀朋友、为人可靠、主动维系友谊而非自我孤立）
- 健康（如：照料健康需求、避开对身体有严重后果的事、以友善的方式爱护身体、摆脱内化的健全主义歧视或肥胖羞辱）
- 屏幕使用时间
- 睡眠
- 饮食、饮酒、药物使用
- 性（如：采取能够提升性体验的行动、与性伴侣公开沟通、以适合自己的方式而非被迫的方式进行性行为、关注性健康）
- 工作或学业（如：完成应尽职责、尽可能摆脱不合适的角色、坚守与他人的健康边界）
- 家庭
- 社会活动或组织工作

—— 你还想在这个列表中添加哪些生活领域？——

1. 在哪些方面我需要对自己更宽容？

1. 我听到了哪些内在的苛刻声音？它们告诉我什么？这些声音听起来像父母、老师、兄弟姐妹、老板、还是过去审判过我的任何其他人？

1. 为什么我难以对自己更宽容些，我在担心什么？

1. 在哪些方面我需要更多严谨？

1. 是什么阻碍了我迈向自己的信念和渴望？

1. 我该如何获得支持以迈出这些步伐？

1. 有没有什么合理的切入点，能让我开启“尺度适中”的严谨，而非基于羞耻和审判的苛责？

关于浪漫关系（或他们所谓的“婚姻”）自助手册的一些注记

基于前文探讨的所有原因，我们确实需要关于性、浪漫和关系的新思维方式，以便停止在彼此身上演练那些制约，停止撕裂朋友圈和社会运动团体。然而，现有的关系自助手册还有很多不足之处。

对于激进主义者来说，流行的这类阅读材料缺乏吸引力且难有大用，主要问题在于：

- 阶级和种族偏见：畅销读物大多是由中上阶层、白人、顺性别异性恋、基督徒编写的，并以这些群体为主要受众目标。许多书籍带有明显的种族主义色彩，仿佛酷儿、跨性别者和穷人并不存在或天生低人一等。

- 刻板教条：大多这类畅销书都坚称维持关系总比离开“更好”，且认为除了终身承诺的一夫一妻制外，任何其他渴望都是“功能失调、自私或不成熟”的表现。

- 过度抬高浪漫爱：预设浪漫关系是满足情感需求的“唯一核心来源”，忽视了友谊的重要性。它也忽视了许多动态不仅发生在浪漫关系中，也发生在朋友、同事和政治创意伙伴之间。

- 伪科学倾向：常用伪科学证据断言性别二元论或浪漫神话是“自然天然的”。

- 污名化神经多样性：将神经多样性视为病态。

- 同化而非颠覆：在评估什么是“好”伴侣、“乖”孩子和“功能正常”的关系时，套用白人、父权、殖民主义、资本主义和健全主义的标准，给出的建议是教你如何“融入”这些系统，而非摧毁它们。

尽管有这些缺陷，标准的关系自助手册中仍有一些有用的见解和工具，但你必须学会“去其糟粕，取其精华”。对许多人来说，阅读这些书籍的过程可能太令人愤怒或具有伤害性。被迫阅读那些忽视你的存在或抹杀你身份的内容，很难让人获得“疗愈”。因此，我在这里分享的是我认为有用的工具，并以我希望看到的方式重新架构了它们。我希望通过重解这些观点 —— 融入女权主义、反资本主义和反种族主义等解放性政治视角 —— 它们能为抗争运动中的人们提供更大的帮助。

[image]

惯习成就自我

“惯习”这个概念能帮我们将日常点滴的行为和感受与生命的宏大轨迹联系起来。

所谓惯习，就是你反复做的任何事。反复做某事会开辟出一条清晰的路径，使这些事变得最容易再次发生。我们的许多惯习都是无意识的，并非真正主动的选择，只是某种机械性的重演。也许在压力下你会走神，或者在冲突中你会感觉僵住无法思考，或者在恐惧时你会下意识反击。这项解放斗争的目标，正是有意识地培养更多新的践行。

当旧的践行过时，不再能匹配我们当下的信念和渴望、甚至导致我们陷入不愿面对的境地时 ——改变就需要主动出击：有意识地选择想要践行新的行为模式。

来自多位老师的这三句话曾带给我强有力的启发：

1. 践行成就你，而且无论如何你都会不断实践下去。

1. 你处理任何事的方式，就是你处理所有事的方式。

1. 你关注什么，什么就会生长。

[image]

你可以问问自己：

我正在一遍又一遍地做着什么，以至于它几乎变成了自动反应？

我可以引入哪些实践，引导我走向我真正想做的事、想要感受到的情绪？

一个很好的例子就是如今的人们与屏幕的关系。

在智能手机时代，大多数人都被大厂的监视资本主义经济体系所操纵、执行着监视资本家和当权者的意愿：频繁拿起手机，哪怕打断重要的谈话和任务也要去查看信息。这分散了人的思维，缩短了注意力。许多人反映，由于长期频繁被打断，他们现在很难长时间阅读、写作或专注于单一任务。57% 的美国人在一年中读不完一本书，却平均每天花 5.4 小时看手机。许多人甚至没意识到自己什么时候拿起了手机，或者在尝试完成复杂任务时不知不觉就溜进了社交媒体。不断重复的打断导致了自动化的行为，最终让人感觉就像是无意识的自主的举动。

心理学研究告诉我们，惯习通过重复形成、并创造大脑中的神经路

径，使人们变得倾向于重复该行为。惯习运作遵循“暗示、惯常行为、奖励”的循环。

1. 暗示：看到手机屏幕跳出通知，或者感到无聊，或者对正在做的任务感到烦躁；潜意识里渴求某种分心。

1. 惯常行为：顺从习惯拿起手机，打开那一系列已经养成习惯的App。

1. 奖励：然后感受到奖励。这种奖励不必是多么好的事（比如看到朋友的信息或心动对象的照片，都算是奖励）。仅仅是打开了那个应用程序、或者随便发现了点什么，甚至只是听到通知铃声响起，就足以触发大脑中的奖励感。

探究人们如何因惯性行为获得回报 —— 即便这种回报并不保证令人愉悦 —— 有助于增强对这些行为的觉察力。同样，留意哪些初始信号会触发惯性行为，也很重要：例如，照镜子可能引发对身体的过度批判。如果能识别这些暗示信号，就能在惯性行为即将启动时及时介入。

比如，你可能有某种“匆忙”的惯性。许多人吃饭非常快，因为他们在上学或上班期间养成了匆忙进食的习惯，现在即使时间充裕也会吃得很快；也许你走路或开车时总是急躁匆忙，即便并没有什么事需要赶，且这会带来压力。再比如，你可能有一种“苛求他人”的习惯，这是从家庭或大众媒体中学来的，例如习惯于批评他人的身材或着装；再或者，你非常擅长观察自己的身体和外表，并在脑海里对自己说一些刻薄的话 …… 你甚至可能不认为这些是被植入的东西，因为这些念头是自动蹦出来的。但就是这些惯习决定了我们的感受、思考、可能性、以及与他人的联结。

[image]

组织、社交团体、和家庭，也都有关于情感的群体规范和践行，且往往是无意识的，

比如匆忙、言过其实、拉帮结派搞小圈子、管理不周杂乱无章、不认

真倾听他人、行事心不在焉、或等级森严 ……

审视 我们如何 独自或作为群体成员 一遍遍践行某些行为、想法和感受， 能为我们想要做出的改变提供一种非常务实的、“下一步小目标”式的方法。

我们中的许多人延续了在家庭中养成的惯习。为了在家庭群体中生存，我们大多承担了有限的角色。也许你是家庭中的照顾者，或者焦虑者，或者是总需要帮助的那个人，或者是躲起来回避问题的那个人。有时你会发现自己在友谊、浪漫关系、工作或社会活动中再次扮演同样的角色。有些家庭惯习可能对人有益并值得保留，但另一些则可能是我们想要摆脱的。这也是为什么回老家会如此困难—— 我们可能会发现自己被推回了那些已经不再适应的旧惯习中、现在感觉格外地不合身。

在面对浪漫关系或性伴侣时，许多人会做出一些不会对普通朋友做的行为和情绪，比如更嫉妒、更具控制欲、更无助、更恐惧、更吝啬、更被动、更具惩罚性或更愤恨。有时这意味着你在自己想要努力“爱”的人面前表现出了“最糟糕的自我”。因为浪漫和性关系往往会激活源自童年的核心不安全感和创伤，个人历史上最艰难的感受和最遗憾的行为往往会出现在这些亲密的关系中。但同时也正因此，这也意味着，这些亲密的关系是审视陈旧惯习、寻找更多选择权的特殊场所。

我们可以将日常生活看作是一系列习得的行为、想法和感受的集合。我的朋友曾告诉我，他觉得他的大脑有磨损的凹槽，就像黑胶唱片的纹路那样。他反复感受过的情绪比其他情绪更容易浮现。我想我们大多数人也是如此。这些“凹槽”是我们更容易跌入的模式，因为它们已经被刻得很深了。

对某些人来说，焦虑会最先浮现；对另些人来说则是愤怒或恐惧。有些人花了太长时间感到自己是异类、孤独或不合群，以至于即使终于加入了一个志同道合的团体，那种“疏离感”也会若隐若现如影随形。这种情况下你会注意到自己在寻找“证据”来证明自己是局外人、证明自己被误解或不被欣赏 —— 大脑在搜寻这种感觉的理由，透过这个滤镜解读一切。这只是说明你对“归属感”的惯习培养不足，所以很难感受到它，即便你很渴望它且机会就在眼前，你也很可能视而不见。

有些人花了太多时间照顾别人的情绪、关注外来的评议，以至于很难接受他人的关怀。有些人则习惯了保持“强硬”或“麻木”，以至于很难允许自己展露脆弱……

你甚至可以将“身份”看作是一套重复的情感、信念和行为 —— 这是女权主义哲学家朱迪斯·巴特勒在 1990 年代提出的著名观点。巴特勒认为，我们的性别是一系列经过重复演绎而形成的表现，而非稳定或自然的生存方式。将身份视为我们“习得”的东西 —— 并且是随着我们在不同空间或生命阶段的习得方式的不同而可能改变的东西 —— 是与性别文化神话的激进决裂。那些神话认为人出生就带有严格的身份类别，并且会“自然地”遵循这些类别的规则，否则就是“出了问题”。

[image]

这个关键观点 —— 身份是重复习得的结果而非自然类别 —— 邀请人们以截然不同的、不那么僵化的方式对待自我认知。

身份往往给人固化的感觉，因为我们被主流文化强行编入了脚本。他人会因为我们是否遵循主流“规范”而给予惩罚或奖励。

我们自己也开始依附于各种身份，以此获得归属感、团结感、被肯定、和联结。这本身没有错，事实上，抗争和团结往往包括自豪地坚持那些被污名化的或“反主流”的“身份”。

但是，如果换个视角：我们的身份 —— 无论是种族、性别、性取向等政治身份，还是基于性格或角色的身份（如领导者、愤怒的人、讲真话的人、总是被冷落的人）—— 都是习得的结果，即使是根深蒂固的新闻也一样，那会发生什么呢？

如果我们认为可以对自己那些看起来“天生如此”的领域带入好奇心、和有意识地改变，生活和关系会发生怎样的变化？

对那些我们被告知是“固定不变”的部分，或者我们所依附的或被困其中的角色，我们能做些什么？

“践行成就你”这个观点可以带来解放。是的，改变惯习很难。但想象我们并非永久性地、被动地被“困住”、并非被彻底“损坏”或“破碎”，可以是一件非常美妙的事。可以尝试新的践行。如果至少偶尔能有不同的体验，或者意识到某个瞬间只是惯习的结果而非注定，我们就会更自由。

这种察觉无意识惯习的工作，是我们在反抗种族主义、性别歧视和残障歧视时渴望社会变革的核心组成部分。你可能会注意到，一些人已经被社会化成自感低人一等且因此不敢分享观点，就此可以通过探索发声的方法让自己感受到生而为人的尊严。你也可能会注意到，另些人被社会化成了自感优越且毫不羞愧地独占空间，于是可以通过主动去练习倾听，在会议或课堂上等待时机再表达。

有人可能被社会化成了期望别人跟在屁股后面打扫，于是可以主动去学习察觉自己是否制造了混乱、或是否参与了清理。主动且努力察觉惯习的模式及其对他人的影响，至关重要。有时，我们还会发展出共享的新习惯，例如现在许多团体在开始时会分享姓名、昵称和角色、以及无障碍需求。这在许多团体中已成为本能，是解决参与障碍的务实方案。第一次尝试新方法时可能觉得新奇或碍手，但只需多重复几次，很快就能自如起来。

[image]

通过问自己：“我正在践行什么？” 来分析自己的行为和情感状态，

能支撑一种信念：随着时间的推移，选择新的行为、新的思考和感受方式是完全可能的。

你也可以在关系中进行这种探究——“我们在一起践行的是什么？”一对伴侣可能会注意到彼此的关系正在使他们孤立，从而共同努力改变这种状况。或者两个朋友可能意识到他们总是关注其中一人的故事，并决定一起来平衡这种注意力失衡。

朋友或恋人也可以选择在生活中增加一些通过协作更容易实现的践行，比如一起阅读、一起看画展、学习烹饪、跳舞或冥想。

改变惯习并不是容易的事。曾经重复得越多，就越容易惯性持续且察觉不到。如果多年来每次看到倒影都在否定自己的外表，改变不会一蹴而就；如果多年来习惯性拖延重要任务，也很难立刻停止。

通常，我们发展出某些惯习是有着极具说服力的理由的，即便它们现在看来是弄巧成拙，但它们形成之初很可能是为了保护我们免受某种伤害。比如许多人受到焦虑的困扰，是因为他们在压力重重的环境中长大，那时为了避免父母发火、为了学业、为了确保账单缴清，在焦虑驱动下行事是生存的关键。现在，即使处于相对安全的环境，他们也无法停止焦虑的侵扰。这些是根深蒂固的思考和感受模式，当我们察觉到它们在生命中重复时，必须对自己保持慈悲。

“践行框架”虽然并不暗示转变轻而易举，但它确实描绘了一种可能性：我们完全可以迈向越来越符合自身价值观和欲望的生活。本书中的许多活动都提供了察觉“自动驾驶”模式的方法，特别是当我们正在演练那些不利于解放或妨碍联结的文化脚本时。最终的目标是选择新的、更有意识的践行，引导我们走向共同的繁荣。

第一章小结

- 我们生活在艰难时期，真的很需要彼此，但我们经常粗鲁对待彼此、并失去联结。

- 糟糕的文化脚本塑造了人们对关系的错误期望，并让人们误以为这些实际上是被灌输的脚本就是“自己的真实感受和欲望”。

- 童年压力、限制和审判（来自家庭、学校、工作、宗教社群等）迫使我们采取应对行为，并形成惯习，这些惯习在日后的关系中可能变得有害。

- 我们的许多想法、感受和行为都是无意识的惯习所践行的，却被误认为是“天生本性”。调查它们，分析它们的由来，能让我们更自主地决定如何生活、如何社交、如何感受。

- 揭穿并打破那些有害的、服务于统治系统的幻象和行为模式，能让我们去追求自己真正坚信的事物和欲望。

[image]

2. 困于自驾模式：在麻木与短暂的亢奋间摇摆

> 在帝国的统治下，感到“幸福”被视为一种义务……帝国……致力于令其臣民受困于“个体化的忧伤”：被禁锢在耗竭心力、充满毒性、且孤立的习惯与关系之中。这种停滞状态可能正是由对“幸福”的追求、以及对痛苦的麻木和逃避，所维持的。相比之下，更充分地活在当下，意味着敏锐地感知影响我们的事物，并积极参与塑造我们的力量。
> —— 卡拉·伯格曼和尼克·蒙哥马利，《快乐的抵抗》（Joyful Militancy）

> 你的心是一块拳头大小的肌肉。保持爱。保持战斗。
> —— 达莉亚·萨蓬-谢文，1999年西雅图反世贸组织抗议活动版画

[image]

有些人担心自己的情感太多、太强烈，觉得自己过于“敏感”；另些人则觉得自己太冷漠，对他人的感受缺乏耐心，或者内心已经有些枯竭。本章将探讨主流文化如何将我们塑造成既麻木（尤其是对自己和他人的痛苦）又永不停歇地追求幻象的人，而这些幻象往往与消费主义和符合社会规范紧密相连。

面对这些压力，我们可以致力于解放自己的感受 —— 摆脱那些告诉我们“该”感受什么、“不该”感受什么的有害脚本。这样做本身就是一种抗争，让我们能更好地应对眼前的处境，洞察现实并采取行动。对我们大多数人而言，这意味着要去感受比被告知的“更多”的东西，夺回我们的情感版图。

本章首先关注“被迫麻木”。在一个充满了损失与苦难的社会里，麻木是维持现状的必需品。这就是为什么精神病学界将“哀恸”列为一种可诊断的疾病。

多年来，精神科医生用于诊断的参考书《精神疾病诊断与统计手册》（DSM）一直在将哀恸日益病理化。DSM 曾经对抑郁症诊断设有“哀恸例外”条款：如果一个人表现出抑郁症状，但在过去一年内经历了重大丧亲之痛，他会被视为正在哀悼，而非患有“心理障碍”。然而，这个时间窗口后来被缩短到了三个月，接着又缩短到了两周。显然，如果你的至亲去世两周后你依然感觉糟糕，精神病学界就会给你的大脑贴上“功能障碍”的标签。

[image]

我们生活在生态危机、战争、警察与边境暴力、大规模枪击、持续的种族灭绝，以及全球和身边社区普遍存在的住房与粮食不安全的条件下 ——

在这种情况下被告知“哀恸是一种病”，简直是 对人格的冒犯 。

我们怎能不哀恸、不悲愤？

然而，职场、医生、和文化机构却告诉人们，哀恸是不合时宜的，甚至是禁忌。

在此背景下，正如心理治疗师弗朗西斯·韦勒所言，选择体验哀恸、忧伤及其他被污名化的感受，本身，就是一种反叛。

去感受这些事物，是为了“抵制保持消极和静止的要求”。

随着我们感受能力的提升，我们也变得更能承载他人强烈的情感，

从而成为深陷困境的社区的 支持源泉 。

接下来，我们将探讨“对自己和他人的痛苦保持麻木”如何催生出一种非此即彼的动态：要么淡化伤害，要么寻求报复。在“弃置文化”中，当我们受伤或发现自己伤害了他人时，我们无法获得尺度适中的体验，而是在“否认坏事发生”和“制造替罪羊进行惩罚”之间来回摆动。

最后，我们将探讨这样一个现象：在当今社会，人们往往需要麻木自己才能生存下来，却偏偏执着于追逐梦幻般的感受，尤其在性和爱情的领域。我们被一种幻想所驱使 —— 相信能通过性与爱情获得“圆满的幸福或惊心动魄的刺激”。许多人通过调情、约炮软件、色情网站、快速地关系升级、沉溺于早已失败的旧情、自我伤害式的暗恋等途径，寻求生化高潮。但建立在追逐快感与浪漫神话幻象之上的情感生活，往往会引发种种困境。本节将探讨如何寻找替代路径，以不受浪漫神话逃避幻想驱动的方式，享受这些活动与情感联结。

[image] “情绪稳定”成为流行词语，甚至成为评判标准，其本身就带着一种令人恐慌的气氛。

在痛苦的世界里靠麻木维生

- 小诺觉得学校很无聊，没多少朋友，和大多数人在一起都感到尴尬。她只有在 Instagram 上跟着健身博主研究塑形方案、或者在满头大汗地完成高强度训练后，才会感觉“良好”。那种筋疲力尽的“成就感”无与伦比。她以为，如果能练成社交媒体上那些人的体型，生活就会变得“更美好”，到那时，她“就能”得到放松并感觉自如了。

- 小扎对世界局势、特别是气候变化感到持续焦虑。他发现自己经常情不自禁地疯狂地刷手机，为了释放压力，他常躲进最爱的电子游戏里玩上几个小时。对他来说，生命似乎只有两种状态：在游戏里充满肾上腺素的兴奋感，或者盯着手机深陷在忧虑和瘫痪中。

- 小艾最近把很多精力从踢球和之前参与的公益项目中抽离出来了。自一年前开始激素替代治疗后，他们在一些社交软件上建立了档案，不断地发信息、调情、寻找约会对象。遇到陌生人的新鲜感、以及发生狂野之事的可能性，促使他们强迫性地查看交友软件、并花数小时安排约会。虽然很多时候事实上很无

聊或令人失望，但当有人对他们的跨性别身体表现出渴望时，他们就会感觉到自己是有魅力的，并急于建立联结。

我们所处的系统希望我们对某些事情保持麻木 —— 麻木到足以在无聊的工作中苦干，麻木到在经历、目睹或参与不公时不会反抗。与此同时，它们操纵我们对喜悦、刺激和联结的渴望，促使我们不停地寻找神话般的“巅峰体验”，比如变富成名、美貌无瑕、或找到完美的性和浪漫。为了在家庭、学校和这个惩罚性的社会中生存，我们关闭了全方位的情感感知。我们中许多人甚至很难知道自己到底感觉如何，也无法认真对待自己（或他人）的情绪。正如弗朗西斯·韦勒观察到的那样，我们拥有一种“失忆和麻醉”的文化 —— 先是遗忘，然后麻木。

对于渴望正义的人来说，这听起来异常熟悉。主流系统假装权力是平衡的，假装现状是公平中立的，假装我们都“应该”只顾自己、“应该”努力攀爬上位。

麻木、分心和遗忘是核心的控制手段，原因如下：

- 看到他人受苦是痛苦的，所以我们保持麻木、见怪不怪。
- 面对 “系统并不公平、非法权威保护一方而打击另一方” 的证据是刺痛的。新闻和社交媒体充斥着令人心碎的消息，我们为自己的感知系统筑起屏障来阻挡这种痛感。
- 当我们的同理心受限时，系统运作效率最高。它 需要 我们扮演支配者、榨取者，或从他人的被奴役中获益。
- 系统希望我们在被针对和被剥削的痛苦中保持麻木，拥有一层“厚脸皮”而不去反抗。我们学会了：为了活下去，感受越少越好。

[image]

整体麻木，却在追逐幻象

为了生存，人们习得了麻木、并成为了事不关己的高手。

在将人们塑造成情感范围狭窄、同理心匮乏的物种之后，这些系统又转过头来向人们兜售“美妙”的承诺 —— 轻松快捷的愉悦感，以及从麻木乏味中逃脱的机会。我们渴望感觉到自己还活着。

我们目睹他人生活的幻象，仿佛他们正沉浸在极致的欢愉中；浪漫电影、歌曲和书籍告诉人们，“爱”意味着愿意为某人而死，失去某人就活不下去，且愿意为对方付出一切。“性”应该是惊天动地的，朋友聚会必须是终生难忘的派对，并产出大把的光鲜照片和爆笑的故事 ……我们看动作片、玩电子游戏、摄入成瘾物质，只为寻找短暂的快感和逃避。我们想要感受，但在经过长期的麻木训练后，如果没有消费体验或扭曲的文化幻想作为“助推”，就很难感受到任何东西。

我们的感受能力与那些使我们麻木的系统紧密相连。追逐消费快感和肾上腺素刺激有时更像是一种麻醉剂，而不是帮助我们连接到真实的生命力。我们被告知，去迪士尼乐园、收到钻石、或在赌场赢钱时，才是“快乐”的。社区教育家塞西尔·安德鲁斯认为，统治阶层正是希望我们既麻木又追逐有限的兴奋感，以便通过消费主义控制我们：

[image]

当我们不再知道自己的感受时，就很容易被“快文化”所操纵：

广告、营销、消费主义、地位、权力 ……

在 内心的空虚 中，我们采纳了 他们想要我们产生 的反应。

操纵者能让我们对各种事物感到兴奋，比如一条牛仔裤、一枚钻戒，或者一个宣称能让你“一夜暴富”的 候选人 。

[image] 2025新年贺词摘选

关注哀恸研究的弗朗西斯·韦勒认为，我们过着“浅薄的生活，被毫无意义的常规和短暂的‘欢愉时光’带来的次级满足感所占据”，因为我们

被社会的生产力指令和物质收益的谎言俘虏了。他认为我们理应活得比这更有活力：

> “我们承袭着非凡的血脉，其中流淌着与野牛、羚羊、乌鸦和夜空亲密共处的记忆……这血脉注定要以惊叹和敬畏之心面对生命，而非屈从与忍耐。” 我们需要经历悲伤和哀愁，才能体会到生命的丰盈。

他观察到，“在哀恸和生命力之间存在着某种奇妙的亲密关系，在看似难以忍受的事物与最精致的生命感之间，存在着某种神圣的交换。” 因为统治系统需要人们麻木，“整个产业都在致力于迟钝和分散人们的感官。我们对麻木的需求植根于对这个社会所提供的贫瘠生存状态的深层不满。”

麻木、焦虑、抑郁、孤立、无聊和断连，成了常态，而我们被教导去追逐那些宣称能缓解生活痛苦的体验和产品。我们表现出的许多强迫性行为 —— 痴迷于暗恋对象、狂刷约会软件、玩游戏、在身体里摄入各种物质、盲目血拼 —— 都是这种 “既麻木又试图感受生命” 模式的一部分。这种动态在社交媒体上最为明显：人们以期待获得认可或关注的方式展示自己，然后强迫性地等待他人分享或点赞时带来的催产素冲击。社交媒体的出现加剧了“个人成名”的幻象。当我们被鼓励追求越来越离谱的认可时，这种专注于外部满足的问题就变得更加严重。

既然我们被告知要透过消费主义幻象来审视生活，那么当我们需要疗愈时，容易被夸大的承诺所诱惑也就不足为奇了。我们被训练成渴望那种快速、奇迹般的且极端的疗愈。各类自助手册承诺让你在短短三十天内变瘦、变富、变快乐、被爱并出名。

而事实上，疗愈是一场终身的旅程，需要去实验各种感受，抵制麻木的压力，并在尝试新践行时直面恐惧。它还要求我们学会接受：我们的许多方面不会改变，尤其不会发生剧烈改变。在此背景下，培养察觉和感受那些微妙事物的能力，是充满力量、具有转化意义且带有反叛色彩的。

[image] 是“你自己的”欲望和情绪，而不是被主流脚本灌输的欲求。仔细分辨这两者至关重要 —— 在被灌输的欲求中，你的所有抉择、

所有焦急和冲动、所有力量和兴致，归根结底，都是被抛弃、被忽视和被排挤的恐惧所驱动的。

培养对微妙和细致的觉知

[image]

在当下环境中，我们被迫经历这两种极端体验。我们对他人之痛麻木不仁，对不公等级制度带来的利益麻木不仁。当自己成为被攻击目标和剥削对象时，我们又对自身痛苦麻木不仁，试图培养"厚脸皮"。这让我们得以在被迫目睹并经历持续不公时生存下去。

与此同时，我们追逐消费文化提供的幻梦 —— 拥有完美身材、顶级服饰、豪车、度假、理想伴侣。我们被灌输这样的信念：这些终将带来幸福，驱散麻木带来的倦怠。我们试图通过电子游戏、暴力电影、药物、追逐性幻想或浪漫幻想等逃避方式，寻求刺激，以此感受自己“活着”。

学习去注意那些被教导要忽略的微妙之处 —— 看起来似乎没什么“赚头”的东西。对别人的感受和经历更具觉知，是否意味着我们要对自己的影响承担更多责任，或者更用心地对待他们？在关注生活的实际感官时，是否会减少追求那些梦幻奖励的时间？与强迫行为带来的极端快感相比，其中的一些感官体验可能显得平淡乏味。我经常听到那些正在戒瘾的人谈到，起初他们害怕如果放弃了某种行为或物质，生活会变得无聊，尽管他们已经意识到这些东西搞砸了生活。他们想知道，如果在这个世界上活着但不再寻找那种“高潮”，会是什么样子？那种对普通现实生活“平庸化”的恐惧是真实的。

[image]

正义与解放事业的许多工作，都在于揭露现实并致力于转化有害的扭曲。

企业希望所有人粘在手机上，不去关注长辈和孩子的故事、季节的更替、候鸟的迁徙。

为了与彼此联结并对现状做出回应，我们需要打破由渴望我们麻木且

成瘾的文化所设定的“感受与不感受”模式。

我们需要重拾与生俱来的感知能力，成为真正懂得情感体验的生物。

[image]

重拾完整的情感谱系

麻木、追逐快感以及失去对微妙感受的觉察，部分表现为我们只剩下一套默认的有限情感，就像玩牌时手里没拿全整副牌。触达更多情绪意味着体验更丰富的人生。

我们中的一些人成长于与成年人互动既不安全又不可预测的环境里，可能因此变得焦虑且警觉，试图讨好成年人以减少他们的情绪大爆发，维持基本生存所需的联结。我们擅长谨慎、感激、羞愧和焦虑，却关掉了愤怒、悲伤和哀恸。另一些人则通过变得强悍、大胆，依靠愤怒、坚忍和鲁莽来应对童年环境，却关掉了恐惧、难过和赞赏。还有人靠着表演“开朗”和取悦他人而活下来，导致长大后很难触及那些被照料者视为“负面”的情绪。

每个人都有某些容易产生的情感，也有某些触不可及的情感。当我们探索这些局限并培养感受全频谱情绪的能力时，我们都能获得与他人更深的联结，并增加安全感和幸福感。

• 哪些情感对你来说最容易产生？
• 哪些情感是禁忌或难以触达？
• 是否有某些情感你听别人谈起过，但你自己从未感受过？
• 你想获得更多触达哪些情感的能力？
• 你是否困在某些情感中想要摆脱？（可参考情绪清单以获得启发。）

培养情感觉知的工具

以下是一些可以增强情感觉知并扩展情感范围的练习：

- 冥想：有助于观察思维、感受和反应的模式。可以帮你与“自动驾驶”反应保持批判性的距离，让你拥有更多的选择。

- 身体疗法和肢体运动：麻木的压力包括对身体感觉的无视。为了在社会控制系统中生存，人们忽略了身体的许多感觉和需求。探索身体的工作方法（可独自进行、也可在专业人士指导下进行）能够增加对身体感官的觉知，帮助我们探索疼痛、羞耻、创伤、愉悦、和疗愈的感受。

- 谈话疗法：提供一个反思感受和经历的空间，审视那些塑造并可能限制了我们情感范围的往事。

- 十二步戒除计划：提供自由的交流空间，听取他人关于酒精、药物、网络、性/浪漫、工作、食物、人际关系危机的感受和经历，并分享你自己的。

- 日记：写下感受有助于更关注涌现的想法和情绪，以及它们与早期形成期经历的联系。

- 学习情感知识：对一些人来说，情感像个谜。通过阅读小说、回忆录、自助手册，收听心理学播客，或倾听朋友描述感受，可以了解他人的感受，并在自己身上寻找类似的感官体验，或察觉到自己无法产生共鸣的地方。其他媒体也能激发情感，比如看悲剧电影练习哭泣，或看自然纪录片观察成年动物和幼崽间的抚育。

- 连接大自然：海洋、群山或天空的辽阔，季节的更替，以及生长、死亡、腐朽和重生的循环，都能帮助我们回归自我，获得反思和微妙的感官体验。

- 艺术实践：资本主义要求我们大多数人在生命早期就关闭创造力。如果没被选为学校里的“小艺术家”，我们就会告诉自己“我”不擅长这个，并停止尝试。只有当我们的创造力能在商业市场上竞争时，才被允许追求它。探索创造力和表达方式可

能让人感到禁忌甚至羞耻，但如果我们能找到进入艺术实践的路径，就会体验到不一样的自我。

情感范围受限的代价

[image]

追求情感觉知是值得的，这能让我们更擅长处理人际关系，并为生存和解放而战。

当一个人缺乏与自身感受的连接时，可能会出现这样的状况：

- 在他人产生强烈情感时感到难以忍受。你可能会给出未经请求的建议，因为你想让对方快点“好起来”，或者主动淡化对方的体验。（“赶紧分了，这种人绝不能要！”；“别矫情了，如今谁不惨啊”；“你情绪这么不稳定怎么行，干不了大事的”……）

- 在自己产生强烈情感时不知所措，忘记如何按照价值观行事。（“看我好欺负是吧?! 心眼好活该当大头吗? 打今儿起老子不做好人了!”）

- 过度顺从他人的强烈情感，随波逐流，即便那完全是过激的、或是在为错误行为辩护。（“移民抢走了你的工作！”；“穷鬼都是卑鄙愚蠢的混蛋，别让他们弄赞了我们的地方……”）

- 当别人的强烈情感针对你时，变得防御或陷入羞耻螺旋，而不是倾听并努力辨别真相。（“女人没一个好东西！”…… 别急，他可能不是针对你，他只是刚刚在一场涉及性别议题的争论中被几个极端保守的观点激怒，还在火头上。）

- 变得回避冲突，避开直接的反馈，转而在背后罗织怨念和八卦；或者在对方提出令自己恐惧的问题时，在重要关系中“人间蒸发”。（“那个谁谁你们知道吧，特别差劲，智障一个……”；“我觉得我们应该坐下来好好谈谈 …… 咦？怎么又消

失了！总是这样，回避型？你准备躲到什么时候！”）

- 撒谎或隐瞒事实，以逃避自己的感受或避开引起他人情绪的后果。（“我挺好的，没有人欺负我，没有歧视 ......”）

尽管每个人都渴望着亲密和联结，但麻木让我们即便获得了亲密也难以持久。

[image]

然而，当我们终于厌倦了戏剧化的冲突循环、厌倦了失去朋友和爱人、厌倦了重复模式带来的挫败感时，冒险去感受更多，就变得值得了。

追求细腻感受实则充满颠覆性和反叛精神，它是立足现实的核心，让我们得以为解放而战。

无法感受就无法真正评估现状、就无法照顾彼此、就无法共同决策，无法践行价值观，也无法对自己和他人负责。

消除麻木、敏锐感知细微之处是终生的修行。这不仅仅是类似于拆除内化的统治系统，更因为拆除内外系统都要求我们具备更强的感受能力。

麻木与情感劳动

女权主义者提醒我们，女性（尤其是有色人种女性）在关系、家庭和组织中往往承担着大量未被察觉、没有报酬的情感劳动。情感劳动是为了维持关系、给他人情感支持、并通过关注人们的感受来维持群体团结而付出的工作。因为在主流社会中，“感受”是不被重视的，但人们依然有情感，所以观察他人的状态、处理社交动态、应对危机等工作，就成了无偿的、不被认可的劳动。

社会期望女性保持敏感并承担这类工作，否则就会面临污名和排斥；

而在男性及广义上的白人群体中，冷漠却被容忍（有时甚至被推崇）。我们可以通过在个人和群体中重视并培养敏感度、情感觉知和情感连接，来改变这种不公平的失衡。我们的疗愈方式是：察觉自己在哪里被变得麻木，并学会将注意力投向那里；同时察觉谁被允许保持麻木，而谁又必须保持高度警觉、关注他人感受以维持运转。主流系统通过性别、种族和其他等级制度来分配这些角色。

[image]

麻木和体面政治

强制性的麻木、匮乏感和物质主义，也与当代对“体面政治”的批判有关。体面政治是一种政治策略，认为争取正义的人应该表现得符合主流的“专业”或“理性”规范。它认为抗争团体应该像公司一样运作，其领导者应该像老板一样行事。

[image]

我们被鼓励 为了富人的资助 、 媒体的关注 、和 非营利机构 的工作而 互相竞争 ，在这些地方，我们 被迫 根据慈善家的喜好来塑造我们的工作。

精英们通过 缩小 我们的诉求、 减少 我们的要求、剔除被污名化和脆弱的群体（ 低端人口 、 移民 、 无家可归者 ），来“奖励”我们。

他们告诉你，想要改变，就需要首先“在谈判桌上占有一席之地”。但要坐上那些桌子，就必须先跪下来围绕着那些本该被拆除的规范和结构来塑造你自己，去模仿那些被视为“专业”的等级规范，把激进锋芒藏起来，去对权力机构说些安抚的话，仿佛那些掌控者只要看到你足够礼貌理性就会改变主意似的……

意识到过去“体面政治”的陷阱，现在的抗争运动正不懈努力地复兴并维持着其他的战斗方式—— 我们自己的方式。

我们培养以透明度为中心的扁平化结构，让我们的团体属于那些参与其中并受工作影响的人—— 他们才是应该做决定的人。我们警惕接受

对手（企业、慈善家、政府）的金钱，警惕向他们的机构求变，更不会试图从内部改变他们。我们很清楚，这些被“认可”和“奖励”的路径，其设计初衷就是为了让任何抗争失效的。

然而，建立扁平、透明、具有转化意义的协作，在实践中是极具挑战性的。无论思想多么激进，也依然被那些将你训练得麻木、不满、追求地位、并沉迷竞争的系统所塑造 —— 这些特征会阻碍人与人之间的连接。对此，必须有意识地实践新型的情感觉知，并建立新技能，以创造我们渴望且需要的运动文化、人际关系和群体。

麻木和微歧视

“微歧视”（Microaggressions）是反种族主义者用来描述在工作、学校、家庭中针对特定身份群体持续发生的微妙、有时是无意的行为。可能是听到一些细微的评价、被冷落、被盯着看，或者是被反复问同样的问题，比如“你从哪儿来？”、“你们这种人怎么做爱？”、或“我能摸摸你的头发吗？”……生活在这样一个人们反复、通常是无意识地强化那些排斥、边缘化和贬低他人的文化脚本的环境中，会对人的生活产生巨大的累积性影响。

微歧视是无休止的，而其意义往往被施害者和目击者淡化。如果受害者抱怨，就会被告知应该“脸皮厚点”，或者被指责“太敏感”、“太易怒/情绪不够稳定”。受到微歧视伤害的人应该被允许感受伤害，并进行投诉，而施害者需要消除麻木，意识到并对自己行为的影响负责。

当有人说我们的行为伤害了他们时，我们受到的训练是去否认，去争辩说“我不是那个意思”。我们不仅被训练去这么说，还被训练去这么感觉 —— 对自己造成的伤害保持麻木，在处于主导地位时对权力动态毫无察觉。

我们害怕被贴上“种族主义者”、“性别歧视者”或“坏人”的标签，这种恐惧让我们害怕去了解自己是如何伤害他人的。要建立一个基于联结关系的新世界，我们必须开启更多的感官体验 —— 包括对这些权力差异存在的哀恸和愤怒 —— 同时也要承受意识到自己处于主导地位、并无意识地演练那些有害脚本时的不适感。如果我们想要解放，就必须保持积极的好奇心，铲除那些让我们在无意中强化等级制度的

文化程序和自动驾驶式的麻木。

关于麻木与追逐幻象的问卷

你会如何麻痹自己？勾选下面所有适用项，并补全。

请注意，这些活动本身都可以是生活的美好组成部分——它们本身没有错——问题在于是否利用它们来麻痹自己，以及在意识到这一点后想采取什么行动。

- □ 网购
- □ 刷约会软件
- □ 沉迷社交媒体
- □ 看电视/刷剧
- □ 看色情片
- □ 蒙头大睡
- □ 聊八卦
- □ 打游戏
- □ 阅读
- □ 运动

- □ 打扫卫生

- —— 还有什么？

如何区分哪些是增强韧性的愉悦放松活动，哪些是在麻木自己 ？当你转向这些活动时，问问自己：

1. 什么样的感受或瞬间让你想要转向它们？（例如：拖延、收到坏消息、担心某事、逃避现实）

1. 过程中和过程后你感觉如何？（例如：更放松了、更有连接感了、更有活力 …… 还是更麻木、焦躁、疲惫、或大脑空白）

1. 你是有意为之吗，还是曾告诉自己不要这么做？它是否干扰了重要的事情，比如正常的睡眠休息、与人交流或完成重要任务？

在高度麻木的生活中，我们许多人以往往不尽如人意的方式追逐“活着的感受”，追逐那些被告知能带来“永久快乐”的东西（事实上，没有什么是永久的）。你是否发现自己以一种失衡的方式、或基于明知虚假的文化理想，在追逐以下事物？

- □ 某种特定身材

- □ 更多的钱

- □ 回头率超高的酷朋友

- □ 最棒的派对

- □ 完美的家

- □ 激情的性爱
- □ 理想的伴侣
- □ 完美的作品（写作、音乐、视觉艺术等）
- □ 完美的工作
- □ 完美的健康和/或体能
- □ 漂亮的衣服
- □ 理想的座驾
- □ 最棒的度假
- —— 还有什么？

然后问问自己：

1. 你是从哪里得到关于这些事物的“正确”或“完美”版本的定义的？

1. 你能否想象在这些领域（家庭、审美、社交、性、健康、交通等）获得更灵活的、不那么受限于僵化标准的满足感？你在生活的其他领域找到了这种灵活性吗？谁能成为你生活中摆脱僵化标准的榜样？

1. 如果放下或减少对上述勾选项的追逐，感觉会是怎样的？你会如何去做？

1. 你是否曾因追求日益升温的性关系或恋爱关系带来的快感，或是为了获得性或情感上的关注，而做过令自己后悔的事？

1. 如果你现在正处于这种状态或考虑这样做，什么能帮到你？

[image]

责任担当：既不淡化，也不惩罚

小安和小芬最近的关系一直很紧张。
他们正在为小芬的祖母提供居家养老服务，而祖母有时对小安很粗鲁，甚至说些歧视女性的话。小安觉得小芬应该出面说点什么，但每当她提起这件事，小芬就显得十分抵触。

两人都很疲惫，繁重的护理工作让她们心力交瘁。小芬觉得小安是在小题大做...
近来，他们发现彼此要么相对无言，要么就为了日常琐事和家务分工吵个不停。

我们生活在这样一个社会里：对于受到伤害的人，往往只有两种反应 —— 要么全盘否定，让受害者闭嘴；要么将伤害者定性为彻底的坏人，必须予以惩罚。

“轻描淡写” 非常普遍 —— 就像小安所经历的，小芬对她关于祖母歧视言论的抱怨嗤之以鼻。由于我们处于这种淡化伤害的文化中，大多数人害怕在遭遇不幸时无人倾听。这可能导致我们对错误保持沉默，或者，让自己变得极度渴望看到施害者受到惩罚，甚至达到了贪得无厌的地步。与此同时，这种动态也让我们自己害怕承认自己的任何错误，害怕被指责、报复和惩罚。这种两极状态其实是一个陷阱 —— 它意味着我们很少能对伤害做出“尺度适中”的回应。

当我们生活在光谱的这两个极端时，缺失的是这样一个现实：所有人都可能会做伤害他人的事，所有人也都可能会经历伤害。

[image]

减少社会伤害的途径，不是严惩少数人而忽视大多数伤害。

相反，我们需要为所有人创造空间，去了解自身行为的影响，

并学习如何不再重复伤害他人的事。

尽管我们可能幻想着惩罚那些做了坏事的人，但事实证明，惩罚式的手段并不奏效。在我们的社会中，大多数造成最严重伤害的人（银行家、警察、CEO、士兵、保护体制化性侵的人）从未受到惩罚。相反，这个世界的惩罚系统针对的是穷人、残障人士、黑人、原住民、无证移民、酷儿或跨性别者。

[image]

在拆除警察和监狱系统的蓬勃运动中，我们也需要拆除内心里的这些观念，

跨越指责和复仇，走向慈悲。

因为我们知道，每个人都会伤害别人，而任何人都可以学会停止这样做。

一个以惩罚为中心的社会需要麻木、防御和复仇。内化这些脚本会损害我们的日常关系，阻碍我们渴望并需要的联结。这并不意味着我们要跳过“感到受伤”的过程，也不意味着受伤时感到愤怒是“不好的”。相反，它意味着我们需要努力从那些关于“好人”与“坏人”的谎言中挣脱出来，正是这些谎言让我们否认许多伤害，或一心寻求惩罚。

我们可以朝着这个方向迈进的一种方式是：提高我们与身边人沟通反馈的能力，哪怕是关于家务、守时、任务执行等微小的冲突和差异。我们越能练习在他人给出反馈时倾听而不轻视，越能练习以慈悲、适度而非寻求报复的方式分享反馈，在面对重大冲突时的调解技能就会越纯熟。

反馈问卷

乐于给予和接受反馈，与我们感受生活、参与抗争运动的能力息息相关。

- 回想一下别人直接给你反馈但结果不佳的一次经历。也许对方言辞犀利，或者你表现得非常抵触。当时哪里出问题了？为什么？

- 回想一下别人直接给你反馈且结果良好的一次经历。也许你学到了一些有用的东西，也许你们的关系因此加深了。当时哪里进行得顺利？

- 回想一下你直接给别人反馈且结果良好的一次经历。当时发生了什么？

- 回想一下你直接给别人反馈但结果不佳的一次经历。当时发生了什么？

- 权力动态会影响反馈。例如，处于主导地位的人（老板、家长、老师、房东）只给反馈却不接受反馈，或者处于从属地位的人害怕说实话会带来后果。在你的人际关系中，哪些最具备双向、直接反馈的可能性？你有什么办法可以增加这种可能性吗？

- 什么能帮你以一种"增强技能、联结、耐力和自我意识"的方式接受反馈？什么能帮助你提供有用的反馈（特别是在存在权力落差的情况下）？你和身边的人如何分享彼此偏好的反馈方式？

- 高频、微小地给出反馈，意味着我们不太可能面临最终爆发的怨恨。这也能锻炼我们划定界限和保持独立个性的能力（详见第四章和第六章）。在日常生活中，你是否可以找人练习分享

一些低成本、微小的反馈？你能明确邀请生活中的某人一起练习吗？

追逐关于性和浪漫的文化幻象

乔喜欢给予和获得关注，经常会对派对上调过情或社交媒体上私信过的人产生强烈的暗恋。
这种情感升温很快 — 只要他对某人产生兴趣，就开始幻想两人的未来。
他会花数小时在网上搜索对方的照片和动态，试图弄清楚对方喜欢谁、喜欢什么。他的约会对象经常觉得他过于热情了，很快就会提出分手。他的朋友们也抱怨乔的感情生活给他们的圈子带来了太多的戏剧性事件。
有时乔也会梦想能和某人约会足够长的时间，长到能让他感到放松和舒适，久到他可以只做自己而不用那么费力表演 …

人的思维模式是长期践行的结果，而践行特定的模式是因为它们曾帮我们度过难关。

主流文化的 “浪漫神话” 传递的信息会让许多人对暗恋对象或想上床的对象产生过度的甚至强迫性的思考。这可能包括过度思考如何让对方喜欢你、如何变得更有吸引力，或者你的暗恋对象/或前任正和谁在一起干什么。性和浪漫成为过度幻想的重灾区是可以理解的 —— 有些幻想让人感觉很好，有些则充满焦虑 —— 因为我们被洗脑了：幻想着情人能让人快乐，误以为有吸引力意味着“有价值”。

对于我们中的一些人来说，逃避现实的思维模式就像一种麻醉剂。工作无聊？看看暗恋对象的朋友圈都发了啥。为钱发愁？研究下改变身材的计划。和朋友吵架？熬夜刷社交软件…… 这种模式 —— 利用某事来逃离当下的处境和感受 —— 可以套用在任何事情上，而性和浪漫相关的事物在此是首选，因为它们承载了太多的文化承诺。在这个世界上，不面对现实往往感觉更安全。我们的身体和大脑进化出了精妙的方法来来帮助逃离现实。

这是强迫行为、成瘾倾向，还是正常现象？

许多人对某些行为和活动存在强迫性依赖。所谓“强迫性”，是指我们想停止或减少它却做不到，或者想要开始一项对健康有益的新活动却无法起步。强迫行为通常是相互关联的，例如对约会和性的过度关注会影响睡眠，因此将它们放在一起思考很有用。

- 在你的生活中，你在哪里看到了这些失衡？（如睡眠、屏幕时间、购物、金钱、学业等）

- 你对此的自我对话是怎样的？换言：你是否在脑海里用尖酸刻薄的话责备自己的这些失衡领域？

- 你会幻想某个特定的人或机构在告诉你什么是“正确”的行为方式吗？你会用这种僵化的标准要求你爱的人吗？

- 你通常做些什么来逃避你想要的改变？是否存在一条通往新行动的折中路径？做出这种改变能带来什么乐趣？

值得注意的是，社会对性有着太多的羞耻感和评判，因此在探究可能的强迫行为时，我们必须非常谨慎。只有当我们自己察觉到某种行为失衡，或者我们想叫停/或想开始却发现做不到时，它才具有强迫性或成瘾性。这可能很难评估：你是否在识别一种真正的失衡，还是仅仅在使用“强迫”这个标签来羞辱自己？找朋友聊聊会有助于理清思绪。

就像上面故事里的乔那样，以失衡的方式追逐这些文化幻象会破坏我们与约会对象和朋友的联结。弄清楚我们是否在以这种方式利用某事，以及这对我们的生活产生了什么影响，是改善关系的基础。

请勿贴标签、不要评判 —— 不要将本书的观点“武器化”

我鼓励你利用本书的内容来理解自己的行为，而不是去审察他人。

我们这个清教徒式的、排斥残障的、刑事化的、种族主义的社会，一直在鼓励我们去归类和评判他人，却剥夺了我们自我反思和自我负责的工具。当别人的行为影响到我们时，做出反应（如限制接触、降低信任、设定界限）是可以的。但是，给自己或他人贴上流行心理学的标签（如“强迫症”、“成瘾者”或“执念狂”等）并不能帮助我们建立所需的关系。更有效的问题是：“他们的行为是否影响到了我，以至于我需要优先考虑自己的福祉？”；以及 “我对自己的福祉负有什么责任，我该如何从这里开始？” 干预和给出反馈有时是合适的，但如果我们先关注自己的感受和反应，这种干预会更有效、更有原则、也更稳健。

主流文化环境迫使我们产生一些应对机制，使我们与愉悦、性、金钱、食物、工作等等关系发生扭曲。因此，可以说大多数人都经历过“强迫”或“成瘾”，或者仅仅是为了生存而必须进行的过度专注或注意力涣散。有害的系统会对某些活动的失衡关系进行评判、贴标签和污名化（如违禁药物），却鼓励对另一些活动的失衡（如工作或健身）；而金钱和特权作为缓冲垫，决定了这种失衡对不同人的破坏程度。有时，我们利用失衡的行为作为逃避的出口，且后果相对较轻。考虑到这一切，在我们的疗愈努力中，将他人贴上“成瘾者”的标签是毫无益处的。

本书的目的不是为寻找问题提供死板的标准。相反，书中的所有观点都是关于如何培养情感技能，以支持我们感受、理解自己的反应、选择互动方式并建立牢固的关系。失衡并没有明确的界线，管理应对机制也没有现成的说明书。我们能做的就是增强感受和选择行动的能力，而不是靠自动驾驶做出反应。通过探究和实践，我们可以提高对自己的责任感，并增加服务于他人的能力 —— 即使我们身边的人正处于危机之中。

[image]

“上头”的感觉

小李晚上睡不着觉，因为他总是在社交软件上流连忘

返，睡得比预想的要晚得多。
起初他给自己设定了限制 — 只联系打算见面的人、不觉得有趣就停止刷屏、午夜后关闭通知 — 但他通常会打破自己的规则，一直熬到凌晨三四点。
他知道自己需要睡眠，但交换照片、寻求并获得关注的那种快感，实在太诱人了。
每当通知铃声响起，他就感觉睡意全无，即使精疲力竭，也无法放下手机去睡觉。

研究表明，调情、性爱、约会、观看色情片、关系升温、刷社交媒体、甚至关于性的谎言，都能让人产生生化快感。由于性行为、坠入爱河的体验，甚至做一些不那么愉快的事情（如强迫性地搜索一个爱而不得的人），大脑中的血清素、多巴胺、催产素等“快乐”化学物质，都会增加。

浪漫神话和反复的践行形成的化学路径，都在训练人的大脑去寻求这种“快感”。我们被条件反射地驱使去追求那些预感会触发“良好”或强烈感受的体验。你是否有任何关于性、约会或关系的行为是受这种“追逐快感”驱动的？ 当我们与暗恋对象眼神接触、写下一段调情的话，或者为了推动关系升温而表白心迹时，都可能获得那种生化上的战栗感。

这些活动带来的快感可以是甜蜜愉悦的，也是生活里正当且美好的部分。但是，如果你做这些事仅仅是为了“爽一下”，哪怕这给生活带来了实际的麻烦或者伤害了别人，那么这种对快感的渴求可能就失衡了。例如，有些人推动关系升温是因为他们沉迷于“被人表白”的快感，但在获得快感后对关系本身并没有真诚的兴趣，这可能会在社群中留下一堆心碎和破灭的期待。或者，像小李那样，虽然没有伤害别人，但因为在软件上寻求认可而牺牲了必要的睡眠，这也会让他感到生活失衡。

追逐快感还可能导致其他后果 ——比如因为太分心去寻找那种好感觉，而搞砸了手边的项目或学业。它也可能导致你并不真正想要的性行为、具有误导性的调情，或者与实际兴趣不成比例的关系跃进。有时我们只想要那种即时的生化冲动，却不想要后续的影响。或许我们已经分不清什么是真正的吸引，什么仅仅是想要那种“上头”的感觉。

正视自己的动机、发现驱动力并检视其对他人的影响，可能会让人感到不适。

追逐快感会产生基于浪漫神话的虚假联结。导致你凭臆想给对方添加光环，以维持获得关注时的兴奋感。同样的，也可能因此把想象出来的屎盆子投射到你想要甩掉的或甩掉了你的人身上。这两种动态都是“通过性与浪漫关注来获得自我价值”这一反应循环的一部分。

[image]

我们中的一些人甚至会为这种追逐快感的行为寻找政治借口。

例如，利用主流文化（或亚文化）的价值观来强推某种关系协议或动态，仅仅是因为想要立刻获得即时满足。

这可能表现为：打着“追求自由自主”的政治承诺旗号，向伴侣施压，要求改变关于与其他约会对象互动的协议，但实际动机只是急于进行某种特定的性或浪漫活动。

或者，它可能表现为按照“浪漫神话”的规范向伴侣施压，要求关系升级（见家长、交换首饰、同居等等）。

在关系中强迫他人做不想做的事总是很糟糕的，尤其是当我们的真实动机与对爱侣所说的话并不一致时。性和浪漫带来的快感发生在一个充满强制性、羞耻感和“正常化”意识形态的雷区，如果我们不意识到自己的动机及其影响，真的会伤害关系中的所有人。

许多人也利用性、调情和约会来感受“自己是有魅力的”。这会使性变成一种表演，一种证明自己价值、确认性别和性身份的方式。当被这种寻求认可的欲望驱动时，许多人会压抑自己的偏好和需求，以呈现一场“被认可的表演”。最糟糕的情况是，这包括做一些自己根本不喜欢、感觉不安全、或事后后悔的事。

别误会 —— 如果想表演，在性爱中进行表演完全没问题，尝试新的性别角色、权力动态和行为可以是解放性的且有趣的。但有时，当性

或亲密关系沦为一种表演，它可能只是在逃避脆弱，是对自我的背叛。检视这些模式并建立清晰的界限，可以帮助我们在这一领域找到更多真正想要的东西。

有些人追逐一整套文化幻想和情感，形成了一种痛苦且可预测的模式 —— 这剥夺了他们关系的独特性 —— 不断地将新面孔塞进同一个“伴侣模版”中。我的一位朋友形容这就像脑子里有一个“男更衣室”。她指的不是洗手间，而是形容她的脑海里总是挤满了某个现任或让她心烦的前任，占据了她大量的注意力。她不断地往里塞人并不解决问题。直到她开始有意识地清空这个空间，才感到巨大的解脱。

结果是，当她摆脱了那些固定的思维习惯后，她能更清晰地看待感兴趣的人。通过觉察那些驱使她建立浪漫关系的潜意识模式，她能够超越掌控她情感和行为的脚本，更准确地看待人和处境。这种转变也能帮助我们更尊重地对待他人，因为我们感知到的是对方真实的样子，而不仅仅是看他们如何适配我们的脚本。

[image]

沉迷于“新关系能量”？

杰西卡·费恩在她的著作《Polywise》中提到，有些人不停地追逐她所谓的“新关系能量”（简称 NRE）—— 即恋爱初期常见的生化和情感快感。NRE 是美妙有趣的，但本质上是短暂的。那些一次又一次寻求这一阶段快感的人往往会留下一堆烂摊子，因为他们在每一段新关系中都极速升温，却毫无疑问地表明，只要短暂的狂喜阶段结束，他们很可能就会立刻抽身离开。

想要短期的关系、或在想分手时就分手，本身并没有错。然而，如果重复这种模式：追逐承诺时的快感，然后在升温带来的“高潮”退去后便抽身离去，这很可能是不道德或不友善的。根据我的经验，大多数陷入这种动态的人并不知道自己在重复某种模式。他们在做那些重大决定时感到“疯狂坠入爱河”，然后在关系遇到一点点困难的时候、或仅仅只是快感消退了，就会感到由衷的沮丧。他们不知道这种情感模式是在追逐升温的快感，而并不是“爱错了人”。有时，需要朋友和社群成员指出这种重复行为及其影响，这类追逐者才能开始看清自己沉迷的模式。

我并不是在争论这些人应该在快感退去后强留，或者完全避免关系升温 —— 而是建议我们大家都能变得更擅长觉察到自己的深层动机和情感习惯。只有理解浪漫神话叙事对我们的掌控，并努力看清自己的感受和行为时，我们才能在任何时长的关系中找到更真实、更基于共识的联结方式。这可能包括检视我们是否在逃避那些伴随冲突而来的情感成长（详见第四章和第五章）。

这种追逐的后果

失衡的追求可能导致许多困扰行为：

- 重色轻友 - 为了约会而放朋友鸽子，将新对象置于一切之上。
- “看我多乖” - 为了新恋人放弃责任或做出冲动决定（如搬到远方或放弃安全套的使用）。
- 装皇 - 在性或约会方面撒谎。
- “快来爱我” - 在对他人并无实际兴趣的情况下寻求关注。
- 被爱的欣慰 - 为了获得关注而与他人约会，并故意误导对方。
- 人设VS.人生 - 为了显得自己有“前卫的性政治”且没有“负面情绪”（如嫉妒）或“需求”（如安全感），而同意自己其实并不想要的协议。
- 空窗期补漏 - 在并没有实际意愿的情况下推动关系升温，进入一段不想做出承诺的关系。
- 得手便下头 - 仅仅为了“上头”而与人升级关系，然后又私下向朋友吐槽对方。

- “窝边草” - 在组织或办公场所追求浪漫联结，而实际上在外部约会可能更有利于环境的和谐。

- 无缝衔接 - 分手后承诺空窗反思，却立刻又卷入新的恋情。

- 狗仔队式追求 - 因为对某人的痴迷而侵犯他人的隐私或界限。

- 情痴 - 分手后情感崩塌，严重干扰日常生活或造成伤害。

- 极品渣 - 突然且在完全没有沟通的情况下甩掉约会对象。

- 亲密鬼打墙 - 在连续的关系中或一段关系内，重复经历升温、狂喜、冲突、分手、崩溃的循环。

- 灾难的前任 - 因为对性或浪漫经历反应强烈，而散布伤害性的八卦。

这个并不完整的清单列出了我们许多人都见证过或亲身经历过的常见行为，在某些圈子里这些行为甚至被视为“正常”。这些行为会导致恋人关系中的孤立，并为伤害和暴力创造条件。有时甚至会导致团体内的冲突，导致成员被排挤，重要的项目和协作流产，甚至使相互依赖的人们陷入长期的反目。

[image]

追逐浪漫神话的幻想和快感会让人们做出后来后悔的不道德行为。“伊卡洛斯计划”（一个致力于消除心理健康污名的同伴支持网络）创建了一个名为“疯狂地图”（**Mad Maps**）的工具，致力于帮助人们为那些被强烈的心理和情感状态吞噬的时刻做好准备。其核心心理念是：在尚未陷入异常的状态下制定计划，然后在需要时执行。

[image]

我建议为你进入的任何强烈状态制作“疯狂地图”—— 无论是强迫性暗恋、分手后的情绪螺旋、新关系的升温过载，还是社交软件带来的迷

糊感。

本书第六章中包含了一个关于“嫉妒”的疯狂地图练习作为示例。如果你已经知道自己重复的某些模式，现在就可以开始制作自己的地图。

本书中的“底线”练习和“约会计划”工具也是将教训转化为具体计划的方法。还有一个基于里德·米哈尔科协议设计的反思工具，适用于那些打算保持“露水情缘”但又陷入严肃联结的人。最后，你将看到一个名为“缓解暗恋或执念七步法”的练习，当你陷入单相思并希望降低情感强度时可运用此法。

[image]

- 你能理解从性、爱情、约会、调情、对感情或前任的痴迷中获得快感的感觉吗？这些思维或行为模式可能对你或他人产生怎样的影响？

- 如果你识别出在这一领域的任何失衡，你认为其驱动因素是什么？

- 在你的生活中，是否有充满爱意且不妄加评判的人，能与你探讨身心失衡的问题，并共同探索本书中的练习与思考？

[image]

—— 未完待续 ——

[image]

[image]

建设中！敬请期待。

截至目前为止，暂时呈现这本书的前两个章节。接下来的其余章节，将在合作方休假结束后陆续呈现。

新春愉快！保持爱，保持战斗力 🍻

[image]
[image]

在激进左翼亚文化中恢复团结：关系结构革命 S11E0N＋1

[image] 关键词

[image] 关联 [image]S11关系结构革命-总章节

[image] Description 关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

创意干预工具包：制止人际暴力实用指南 - 关系结构革命 S11E0N

[image] 关键词

[image] 关联

[image]S11关系结构革命-总章节

[image] **Description**

关系结构革命

[image]

[image]

建设中！敬请期待。

[image]
[image]

[image]
关键词
[image] 结构革命
Description

[image]
[image]

[image] 关键词	互助 性暴力 自治
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] **Description**	结构革命

[image]
[image]

[image] 关键词	亲密关系 性关系
[image] 关联	[image]S09超越米兔-总章节: 解决我们之间的问题，同时不给敌人制造机会
[image] **Description**	结构革命

[image]
[image]

[image]

关键词

[image] 结构革命

Description

[image]

操作安全性 - Digital Security

"永远不要把思想和行动分开，不要把我们知道的东西、我们理解的东西和我们做的东西、我们采取行动的东西分开"。 —— 阿尔弗雷多·M·博南诺

[image]
[image]

使用Tor保护自己时千万不要做这9件事

[image] 关键词	tor 数字足迹 自检
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2018年5月3日
[image] **Description**	操作安全性

我们利用代理服务器来满足匿名需求，在互联网上保护自己的隐私，避免被追踪。Tor 是所有工具中级别最高的，洋葱路由器项目被认为是那些想在互联网上隐身的人的最佳选择。

- Table of Contents

1.请勿将您的 手机 在 **Tor** 上用于两步验证：
2、 不要 在 **TOR** 之外操作用户帐户：
3、不要发布有关您的任何 个人信息 ：
4、不要通过 **TOR** 发送 未加密 的数据
5、 不要 在 **Windows** 中使用 **TOR**
6、不要忘记 删除 **cookies** 和本地网站数据
7. 请勿 将 **TOR** 用于 **Google** 搜索
8. 不要 在 **TOR** 上打开 **HTTP** 网站
9、 不要同时 使用 **Tor** 和不使用 **Tor** 访问同一台服务器

[image]

关于 Tor 本网的详细介绍和分析：

1、Tor 项目的由来：https://steemit.com/crypto/@iyouport/3jeanq；

2、反侦察： https://steemit.com/crypto/@iyouport/2mws67 ；

3、注意事项： https://steemit.com/crypto/@iyouport/64ra5i ；

4、原则：https://pao-pao.net/article/1030

洋葱路由有能力保护您，让您远离那些在互联网上试图追随您的纠缠者和邪恶的权力。即使您想成为另一个斯诺登，也可以通过使用 TOR 浏览器来做到这一点。

Tor 浏览器旨在尽量减少间谍行为和窃听的机会。当然没什么是完美的，Tor 也有它的缺点，问题会出在出口节点上。但是 Tor 无疑是我们目前能拥有的最佳选择。但建议您不要混淆 Tor 的默认设置，除非您知道自己在做什么。这是因为启用 **Javascript** 和其他插件可能会导致您的 **IP** 地址被泄漏。

洋葱路由器的普及激发了一些居心不良的人，创建恶意软件并使其看起来很像 Tor 浏览器。这是用户应该担心的事。

此外，无论你认为自己有多安全，你都不能对这样一个事实视而不见：你的任何一点错误都将有可能在互联网上泄露你的身份。

这里有九件事，在使用 Tor 的时候你不应该做：

1.请勿将您的 手机 在 **Tor** 上用于两步验证：

大多数网站会使用手机号码进行两步验证，将OTP（一次性密码）发送到您的手机上，使您可以安全地登录到自己的帐户。但千万不要在 Tor 浏览器上这样做。如果您将手机号码提供给网站，它只会在网上妨碍您的匿名状态，因为使用手机号码更容易追踪您。

请注意，即使您使用的是以其他人的名字注册的 **SIM** 卡（非实名手机卡），电信运营商也同样可以轻松追踪到您，因为他们可以将设备的 **IMEI** 号码保存在其数据库中 —— IMEI 号码是独一无二的，也就是说不会出现两台设备共享相同一个 IMEI 或 MEID 号码的情况，那就是您的身份。

2、 不要 在 **TOR** 之外操作用户帐户：

如果您使用 TOR 浏览器登陆您的 Facebook，Twitter 或电子邮件帐户，就请不要在 TOR 浏览器之外使用这些帐户，因为它会将您的在线身份暴露给网站。

网络上的几乎每个站点都会记录登录和注销时间、您的位置、IP 地址和其他详细信息，在开放的互联网上使用您的帐户即使一次也足以让您的 **IP** 地址被记录，并最终暴露您的身份。

3、不要发布有关您的任何 个人信息 ：

必须牢记这点，不要在使用 TOR 时发布任何个人信息，如姓名，地址，生日，信用卡号码等等，它将揭示你的身份，造成使用 TOR 也没有意义，希望你能理解。

为了让自己完全隐藏起来，你需要伪装自己。这意味着您需要在使用 **TOR** 时将自己表现为具有不同行为特征的人。变成完全不同的人，具有不同的好恶、选择偏好，以及理想等等。

为此，请使用新的电子邮件地址创建一个新的用户帐户，该电子邮件地址必需不会反映您的真实身份。将其用于您的社交媒体账户。

另外，不要混淆匿名和假名。匿名连接是您想要连接的服务器不知道您的真实 IP 地址/位置和您的身份的相关性。

假名连接是被请求的服务器不知道你的实际 IP 地址/位置，但是它可以知道与连接关联的身份，虽然那个身份不是你。

4、不要通过 TOR 发送 未加密 的数据

阅读上述我们的文章您会发现，TOR 加密的是你的连接而不是你的数据，而 TOR 的出口节点是脆弱的。因此，强烈建议不要通过 **TOR** 网发送未加密的数据，因为有人可能会守在出口节点访问您的信息。你不知道那会是谁。

5、 不要 在 Windows 中使用 TOR

微软的 Windows 是世界上使用最多的台式机操作系统，但是当你想要使用 TOR 浏览器时，它可不是什么好的选择。

Windows 无法被信任是由于操作系统本身存在的漏洞，即使您使用 TOR 访问互联网，也可能会泄露您的身份。

Linux 系统将为您提供良好的服务。像 **Tails** 和 **Whonix** 这样的 **Linux** 发行版都预先配置了 **TOR**。您也可以在任何您喜欢的发行版上手动配置它。

6、不要忘记 删除 cookies 和本地网站数据

当您访问网站时，它会向您的计算机发送一个小文件，以保存您的浏览习惯和其他数据的记录，以便网站在您下次访问时能够识别您，该文件称为 cookie。某些网站也可能将数据本地存储在您的硬盘上。

在 TOR 上执行的每个浏览会话之后，您应该删除这些 cookie 文件和本地网站数据。这些东西可能会让网站收集到有关您的信息并跟踪您的位置和 IP 地址。

Tor 浏览器的更新版本会在结束会话后自动删除网站 Cookie 和下载历史记录。另外您也可以单击新建标识选项（在地址栏之前单击洋葱按钮），而不必关闭 Tor 浏览器。

7. 请勿 将 TOR 用于 Google 搜索

如果您想在使用 TOR 时保持匿名，请勿使用 Google 搜索。虽然这听起来很奇怪，但这是因为 Google 会收集您的搜索请求等信息，将 Cookie 文件存储在您的计算机上，并跟踪您的浏览习惯以支持其广告服务。

你肯定不想透露这些信息，因此，您最好避免 **Google**，使用其他搜索引擎，如 **DuckDuckGo** 和 **StartPage**，因为它们不会记录您的 **IP** 地址或任何其他活动。而谷歌有可能会显示一条错误消息或要求验证码，这是因为通过 Tor 访问 Google 的人似乎很可疑。

8. 不要 在 TOR 上打开 HTTP 网站

如果您使用 TOR 访问 HTTP 站点，有人可能会在出口节点上访问您的信息。传输到 HTTP 站点和从 HTTP 站点传输的数据是未加密的，并且可以在端点上进行查看，因为 TOR 仅加密其网络内的连接。

您可以通过使用 HTTPS 来防止这种情况。他们使用 SSL（安全套接层协议）和TLS（传输层安全协议）等端到端加密协议。因此，即使您位于 TOR 网络之外，您的所有数据仍然安全。

9、 不要同时 使用 Tor 和不使用 Tor 访问同一台服务器

这是你必需记住的一件重要的事。如果您使用TOR（匿名）访问特定的远程服务器，就切记不要从 TOR 网外（非匿名）访问同一台服务器，因为这可能会导致您的实际身份被揭示。

这是因为，如果你的网络出现故障，你的所有连接将在同一时刻终

止，如果有人对你进行窥探，并完成拼图，这一点都不难。

此外，Web 服务器可能会尝试通过增加或减少 TOR 或非 TOR 连接的速度来将两个连接关联起来，以查看速度是否在另一个连接上存在波动，从而跟踪您的真实 IP 地址。

[image]
[image]

如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？

[image] 关键词	传输安全 街头 通信
[image] 关联	[image]黄貂鱼
[image] 创建时间	2018年11月1日
[image] **Description**	操作安全性

拦路扫描是相比下很笨拙的监视手段。明明有很多可以让当权者轻松监视所有人的技术工具，他们为什么不用？更有可能的是，他们一直都在使用，只是我们不知道。

- Table of Contents

[image]

2018年网络曾经传出消息称中国北京出现了警方在街头随机扫描路人手机的审查监视行为。我们没能具体核实该消息，包括它出现在哪些地区、扫描是否有针对性、以及该扫描技术本身的用意是什么。但此前新疆地区曾发生过同样的事件描述，据称针对移动设备上安装的反审查软件。

不管怎样这种强行扫描的做法是非常笨拙的，因为显然有很多其他技术能够让当权者在公民完全不知情的情况下实现间谍式监视，IMSI 捕手就是。

IMSI 捕手（俗称黄貂鱼）这种秘密手机监控技术的使用近几年来已经

变得非常常见，很多国家的政府和情报机构都在使用这种技术监视他们的公民：英国警方前段时间一直在因使用 IMSI 捕手被民间权利组织挑战；美国两年前就被曝花费了上亿美元购买 IMSI 捕手，警方和情报部门利用这种技术在没有法庭手令的情况下进行大规模监视；加拿大警方公开将 IMSI 捕手描述为“重要工具”；2015 年伊朗将黄貂鱼送给了穆加贝，此后津巴布韦一直在使用它监视社会……

美国使用黄貂鱼的最新报告，以及公民社会的反抗《How the cops are tracking you》

另参见以下报告：

- **Associated Press: US suspects cellphone spying devices in DC, Frank Bajak, 2018.04.04**: https://apnews.com/d716aac4ad744b4cae3c6b13dce12d7e/APNewsBreak:-US-suspects-cellphone-spying-devices-in-DC

- **NPR: Feds Say They've Detected Apparent Rogue Spy Devices In D.C., Merrit Kennedy, 2018.04.04**: https://www.npr.org/sections/thetwo-way/2018/04/04/599428495/feds-say-theyve-detected-apparent-rogue-spy-devices-in-d-c

- **Washington Post: DHS has detected possible cellphone surveillance in D.C.—and doesn't know who's doing it, Matt Zapotosky, 2018.04.03**: https://www.washingtonpost.com/world/national-security/dhs-says-it-has-detected-possible-cellphone-surveillance-in-dc–and-doesnt-know-whos-doing-it/2018/04/03/f69fbe36-3785-11e8-acd5-35eac230e514_story.html

- **BBC: Mystery Stingray devices discovered in Washington, 2018.04.04**: http://www.bbc.com/news/technology-43639709

- **MuckRock: Rochester police release unredacted list of**

Harris Corp StingRay and KingFish products, Curtis Waltman, 2016.12.02: https://www.muckrock.com/news/archives/2016/dec/07/rochester-police-release-unredacted-list-harris-co/

- **Electronic Frontier Foundation: One Pager on Cell Site Simulators**, https://www.eff.org/document/eff-one-pager-cell-site-simulators

- **New York Times: New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says, Joseph Goldstein, 2016.02.11**: https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html

- **American Civil Liberties Union: Stingray tracking devices: who's got them? Updated March 2018**: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them

- **DHS Letter Cover**: https://www.documentcloud.org/documents/4429966-DHS-response-to-Wyden-3-26-18.html

- **DHS Letter Attachment**: https://www.documentcloud.org/documents/4430049-DHS-attachment-in-response-to-Wyden-3-26-18.html

我们在此前的一份详细报告中介绍过 IMSI 捕手 https://iyouport.substack.com/p/lr--bc3?utm_source=publication-search。2016 年的欧洲黑帽会议上，研究人员公开展示了这种通过 WiFi 操作的 IMSI 捕捉器攻击方式，允许攻击者在一秒钟内捕获智能手机的 IMSI 号码，然后利用该 IMSI 号码来跟踪监视移动设备用户。

一些比较知名的 IMSI 捕手是 Harris 公司的 StingRay，KingFish，和 Hailstorm，以及波音/数字接收器技术公司的 DRTbox。这些假基站

通常放置在车辆中，甚至装载到有人驾驶和无人驾驶飞机上。

上述这份报告同时介绍了很多监视技术工具，所有素材均来自一次展示会：英国政府汇集了数百家监视技术公司，展示他们的全方位监视能力，从天空到地下到街头几乎无所不包，并且我们专注于其中每一项技术在中国的使用情况。结果发现，中国几乎全部拥有，并找到了准确报道证实其已被布设，唯独黄貂鱼 —— 中国没有公开声称使用这种技术，然而它是如此的简单和具有普遍性，你能想象中国不会用吗？

IMSI 全称“ international mobile subscriber identity ”（国际移动用户识别码）是区别移动用户的标志，储存在 SIM 卡中，可用于区别移动用户的有效信息。不要将 IMSI 号码与 IMEI 号码混淆，IMSI 直接绑定到用户，而 IMEI 绑定到设备。

Wi-Fi 网络可以捕获附近智能手机的 IMSI 号码，无线跟踪并监控用户的根源在于智能手机（包括 Android 和 iOS 设备）连接 Wi-Fi 网络的方式。

在大多数现代移动操作系统中有两种广泛实现的协议：可扩展认证协议（EAP）、认证和密钥协商（AKA）协议。这些协议允许智能手机通过自身设备的 IMSI 号码切换登录到已知的 Wi-Fi 网络，实现 WiFi 网络自动连接而无需所有者交互。攻击者可利用 WiFi 认证协议的这种机制伪装成 WiFi 网络，诱骗智能手机连接、捕获 IMSI 号码，从而实现对用户的跟踪监视。

此外攻击者还可利用捕获的 IMSI 号码实现移动运营商提供的 WiFi 呼叫功能。智能手机 WiFi 呼叫功能允许用户通过使用加密的 IPSec 协议连接运营商的边缘分组数据网关（EPDG）。在这个过程中用于验证 WiFi 呼叫的互联网密钥交换（IKEv2）协议也是基于 IMSI 号码，这可导致发生中间人（**MITM**）攻击，允许攻击者拦截通信流量。

听起来似乎很可怕，尤其是在考虑到对技术不熟悉的人占据绝大多数的情况下。如今恶性局面已经到来，我们除了普及应对技术之外别无他法。我们当然应该去追求技术的简单易用，让安全惠及大众，但有些时候，最大的难度在于如何有效地提醒大众对安全的重视。

在安全的角度看来，IMSI 捕手之所以邪恶是因为其侵犯完全在不知不觉中，而不是像中国当局所采取的拦路扫描那么直观。对于后者，大多数时候你能想到办法躲开，因为眼睛就能给你一个预警。但是在中国社会的习惯性思维角度上看，显然是拦路扫描更“有效”，正因为它将震慑直观化了。震慑才是根本性目的，在充满恐惧的社会里这种方法非常有效。

理论上中国当局的做法明显“帮助”了提升中国社会对安全问题的重视。只要能重视起来，简单的学习就可以掌握基本的反监视能力。但是现实层面上我们不得不考虑中国社会普遍的畏惧心理，它才是最大的障碍。Snowden 说：“权利的争取来自于战斗，除非你先站起来，否则赢不了”。希望中国社会能理解这句话的意思，顺服将让你永远都无法获得自由。

说多了。下面首先介绍一个相对简单的方法，以应付黄貂鱼。

这东西叫 **SnoopSnitch**。

SnoopSnitch 是一个 Android 应用，它会收集和分析移动基站数据，让你可以充分意识到移动网络的安全性，并给你提供一些伪基站、用户跟踪和 OTA 更新的警告信息。你可以使用来自 GSMMAP.org 上收集的 GSM 安全地图数据，同时也可以给该网站贡献数据。

[image]

SnoopSnitch 项目由德国安全研究人员三人组成，即 Alex Senier，Karsten Nohl 和来自 SRLabs 的 Tobias Engel 。它在 Android 平台上推出。点击此处从 Google Play 商店下载 SnoopSnitch 应用。

SnoopSnitch 收集并分析移动数据，让您了解移动网络安全状况，并警示您防范各类威胁，例如伪基站（IMSI捕获器）、用户追踪以及远程升级。

目前，SnoopSnitch 仅与配备 Qualcomm 芯片组和现有 Android ROM 或具有 Qualcomm DIAG 驱动程序的任何适当自定义 ROM 的

Android 手机兼容。收集移动网络数据需要 **root** 权限。

虽然此应用程序无法保护您的手机不被黄貂鱼咬住，但它至少可以通知并提醒您特定区域内是否存在监控系统。

在下面视频中观看 SnoopSnitch 的演示；并在这里看到更多详细介绍：

https://youtu.be/kSGwxg3vI9g

反监视方案不止这一种。有几种闭源硬件解决方案都可用，但有点贵，幸运的是还存在免费和开源的软件和硬件解决方案。

另一个旨在检测 IMSI 捕获器的开源软件项目是 **AIMSICD**（Android IMSI 捕手检测器）。

AIMSICD 自 2012 年以来一直处于开发阶段，它仍然是实验性软件，并且仍处于 alpha 开发阶段。用户应该有心理准备它可能会出现一些误报和虚假警报。该应用程序无法从 Google Play 商店获得，但可以从 GitHub，F-Droid 和 Aptoide 下载。

AIMSIC 尝试通过各种不同的方法检测和避免 IMSI 捕获器，包括检查塔信息的一致性，监控信号强度，检测 FemtoCells 以及静默 SMS。该应用程序还可以帮助用户避免使用不良加密或根本不使用加密的合法蜂窝基站。应用程序使用六种颜色编码的图标来显示当前的威胁级别。

- 当 AIMSICD 显示绿色图标时，表示未检测到任何威胁，并且正在使用 A5/3 加密或更高；
- 正在显示黄色图标时表示中等威胁级别，警告使用的是较不安全的加密；
- 高威胁级别由橙色图标表示，这意味着 IMSI 捕获器正在主动跟踪该区域内所有用户；

- 红色图标提醒用户威胁级别是危险，表示已经检测到 IMSI 捕获器正在主动跟踪您的设备；

- 该应用程序还有一个黑色图标具有骷髅头，意味着您的设备正在被远程操纵。

AIMSICD 从 OpenCellID 收集蜂窝塔的位置信息，然而，OpenCellID 项目正在关闭，当前的维护者在寻找其他人来维护它。似乎 AIMSICD 尚未发布更新，更新应该能实现用于蜂窝塔位置信息的另一项服务。

AIMSICD 需要一个 **root** 的 **Android** 设备才能正常运行。

StingWatch 是 Android 的另一款旨在检测 IMSI 捕手的应用程序，并且不需要 **root** 设备。与 AIMSICD 一样，StingWatch 也是一款免费的开源软件解决方案，用于检测 StingRay 等设备，但与 AIMSICD 不同，StingWatch 可在 Google Play 商店中获得。

还有一个解决方案是由网络安全先驱 John McAfee 开发的专有应用程序 DVasive Pro，该应用程序不是免费的。DVasive Pro 允许用户锁定他们的手机无线电发射器和接收器。

华盛顿大学安全研究人员开发 了一种名为 SeaGlass 的新系统，也是用来检测威胁的。去年 SeaGlass 传感器被安装在西雅图和密尔沃基的15辆汽车中，结果研究人员发现了数十种异常情况。这种东西很适合装在汽车里，理想情况是那种长时间行驶穿越城市大街小巷的汽车，它会随时汇总数据并构成基线图。

[image] SeaGlass

[image]

用户自己可以采取的保护蜂窝通信私密性的另一个步骤是使用 Signal 和 Tox 等加密通信应用，并使用安全的 VPN 或 Tor 加密其蜂窝互联网流量。

虽然IMSI捕手仍将拦截数据包，但数据加密了，防止攻击者获取对通信内容的访问权限。

世界各地的活动家们一直在反对这种在全国范围内大规模侵犯隐私权的行为，推动通过地方和州一级的立法，禁止使用它、或者提供有效的公民监督。中国没有公民社会和隐私活动家，于是反监视的工作更多需要每个人自己动手。

还是那句话，首先应该重视起来，要知道这种威胁已经无处不在。

以上只是相关反监视技术中的几种，如果您还有其他办法，欢迎尽力传播。

[image]
[image]

使用社交媒体时你必须注意什么？—— 更安全的抵抗

[image] 关键词	个人 反监视 社交媒体
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人 ；[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法 ；[image]S01整体安全 - 总章节：前线安防入门课
[image] 创建时间	2018年11月29日
[image] **Description**	操作安全性

异议和反对是完全不同的。做异议非常简单，你只需要说出“我不同意什么”；而反对，您就需要更多更充分的技巧和技术能力。而其中最为基础的就是：保护自己的能力。

- Table of Contents
安全的基本原则
区域化规则
隐藏规则
至少应该知道：**Twitter** 的风险
技巧的获得重在实践
破坏安全的对手
心理健康风险

[image]

参与政治活动、甚至仅仅是关心政治话题，在这个时代都有可能迅速令你面临风险，包括并不限于生活、职业、工作和人身安危，并且审查红线是模糊的，多数情况下你可能完全不知道自己究竟哪一句话招致了灾难。

事实上，这种局面在全球所有国家都一样，只是审查标准不同。最初被大众捧为变革契机的社交媒体，被证明只是个巨型的监视器，而且是史上最具侵入性的监视器。之所以变成这样，很大程度上是由于有太多人不重视使用社交媒体的基本安全性。

在中国，关注隐私安全的人们已经开始嘲笑那些追求上网实名制的异议人士，但似乎整体上没有什么改观，或者为时已晚；更为重要的是，仅仅换一个化名是远远不够的，社交媒体有太多数据可以轻松确定你的身份。并且，对这些数据调用以跟踪异议人士、活动家和记者等敏感群体的政府行为，一直都在全球各个国家通用。

鉴于中国当局非常善于模仿、并且严重不透明，大型科技公司同样严重不透明（所谓的透明度报告早已形同虚设）不只有 BAT，还有硅谷巨头公司对中国市场的垂涎，中文用户真的非常有必要提高警惕，即 根据全球不同国家出现的监视追踪案例和最新间谍跟踪技术的披露，将其全部假设为中国也会使用。借此思考应对方案，以便在最大程度上避免措手不及。

并且，任何时候，公开的抗议对于政治合法性来说都是至关重要的，信息的流通对公民行动和认知具有决定性意义。自我审查是必需被否定的，我们的目标应该是自由的发言、无障碍的信息交互、无跟踪的网络动员和集结、以及每个人的安全。

[image]

如您所知，我们一直在支持去中心化网络模式，鼓励人们离开这些不透明的巨头提供的服务。但我们知道，这很可能是个长久的工作，巨头的服务已经深入每个人生活的方方面面，习惯是顽固的很难改变（我们将在后面的文章中详细分析这些问题）。于是，短期内急需提请所有人关注的重点就是，继续使用 Twitter/X 等服务时，您最基本应该注意什么。

我们依然不建议完全放弃在线的动员和联合，毕竟暂时看起来它依然颇具效率，并且希望能充分利用互联网这一能力。

本指南希望有助于降低个人所面临的人身风险，同时赋予人们安全行动的能力。

互联网没有国界，技术没有国界，这些保护方案在所有国家都是通用的。

[image]

激进派社区用户请从这里进入：[image]数字技术限制和最佳实践

安全的基本原则

操作安全性的基本原则实际上非常简单，就是我们常说的三个C：

- Cover
- Concealment
- Compartmentation

当然，还有更多更为严肃的反间谍技巧，我们曾经介绍过一些，但要记住这三个概念，它们是最基本的、也是必需的。其中最重要的是compartmentation 和 concealment，在实践中，这意味着您需要将您的具有敏感性的社交媒体帐户与您的个人真实生活完全分开。

区域化规则

1、🔐 要 —— 为此敏感社交媒体帐户专门创建一个新的唯一电子邮

件地址。

这里有很多选择，但请认真考虑使用非本土的服务；访问此帐户时始终使用 Tor，除了发布异议和反对信息或观点之外，永远不要使用它发布其他内容。

这不是废话，我们曾经观察到有中文 Twitter 用户在简介中写着自己的 QQ 号、手机号、163邮箱。这是很危险的。

[image]

返回：[image]使用Tor保护自己时千万不要做这9件事

2、🔐 要 —— Twitter 是一个收集电话号码的蠢货，你很难在不提供电话号码的情况下使用它。

您需要一个一次性的预付费电话，或获得一次性 VoIP 号码。

这种方法对于其他需要关联手机号的通讯应用也都需要，详见下文：（如果您在美国的话，我们严重不建议使用谷歌语音，因为已经有很多案例显示它容易很受到州级政府的攻击，其他服务也有可能）

[image]

返回：[image]虚拟手机号和马甲邮箱隐藏真实信息

返回：[image]移动网络运营商

返回：[image]匿名手机

3、🔐要—— 使用 Tor 创建您的 Twitter 帐户，以及对 Twitter 帐户的所有访问权限；IP 地址以及 cookie 和其他跟踪器，Twitter 都有；这些数据也可被调查记者和媒体使用。

4、不要**!——** 不要使用您的智能手机应用程序登录该敏感社交媒体帐户。

否则 IP 地址将直接链接到您的电话帐户，并且您将面临通过技术手段被曝光的高风险；

如果您必须在手机上使用 Twitter，请将其设为仅适用于该帐户的专用手机，而没有其他信息（如个人通讯录、照片等）。

此外，Tor 的安卓版已出，它是个好主意，IOS 版很快会能实现；如果你是技术人员，我们推荐 **Algo;** 如果不是技术人员，那么请使用 **Freedome**，都可以尽量减少暴露。

5、不要**!——** 该敏感账户不要响应 **DM** 或直接回复，特别是如果有 URL 的话（可用于捕获您的 IP 地址）甚至利用您的设备。

说真的，不要点击通过@或 DM 发送给你的链接，特别是短链接。

不过值得指出的是，Twitter 上的所有网址都是通过 Twitter 自己的 t.co 缩短和分析重定向的，因此即使来自已知且受信任的“安全网址”也会暴露帐户 IP。

6、不要**!——** 不要让这个敏感账户与您的个人帐户或与您相关联的其他人的帐户进行互动。

一般来说，尝试维护单一的信息流，将数据推送到公众，不参与讨论或在帐户上涉及任何有可能关系到“私人”的信息。

Twitter 上没有隐私，与你成为朋友的人也可能是被派去监视你的人。

您不需要增加这样的风险。

7、不要!—— 不要让这个敏感账户关注您的私人账户，或者任何与您有关联的账户，如果必需关注一些账户的话，仅仅关注通用账户，比如认证的媒体和组织。

8、不要!—— 不要从您的敏感帐户中推送“个人”照片。这包括屏幕截图、或任何个人性质的内容！

如果需要包含图片，请将其裁剪，以便无法看到网络或其他浏览器标签等重要细节信息。

任何时候，上传之前抹去元数据！

9、不要!—— 请确保您的头像不是您的自拍或者您的亲属和亲密朋友的照片；确保简介信息与您私人没有任何关系。

隐藏规则

1、不要!—— 不要向任何人展示或介绍你的活动，甚至不要提示这点。

无论你在私人生活中采取什么样的公开立场，例如参加游行或集会、签署请愿书、或参与抵抗运动，都不要告诉任何人关于您的这个敏感 Twitter 账户。是任何人！包括你的伴侣、你的孩子、你最好的朋友和同事，保密的第一条原则就是保守秘密。

2、不要!—— 任何时候不要使用工作单位的计算机（和单位的网络！）登录这个敏感账户。因为你无法控制它们，它们可以在未经你许可的情况下被查封和搜查；它们也有可能正在运行由您的公司/代理商安装的间谍软件，来监控您的活动，并确保您不会浪费时间在 Twitter 或 Medium 等网络应用上。所以它也能发现你正在做什么。

3、🔐 要—— 通过启用全盘加密、使用强密码、使用密码管理器（在本地存储数据，而不是在所谓的云中存储数据）来保护您的设

备；快速安装补丁；如果违反了上述建议您实际在使用智能手机操作您的敏感 Twitter 帐户—请勿使用指纹解锁和面部解锁！

4、🔐 要—— 在操作敏感账户时，改变您的写作风格。感叹词、破折号、惊叹号、省略号等等细节的频率，都有可能暴露您的身份。通过行文推测笔者身份的技巧是行为心理学的一个基本功。它并没有你想象中那么复杂，大多数做过十年以上编辑工作的人都能自动获得这种能力。

5、不要❗—— 不要使用这个敏感账户与您的任何朋友互动、包括任何熟人，不要让该账户与您的任何真实生活发生哪怕一点点联系。

时刻记住，有人在长期暗中观察该账户，搜罗这些细节信息，此人就是有能力把你扔进监狱的人。

至少应该知道：Twitter 的风险

作为一种 Web 服务，Twitter 收集（并从数据代理商处购买）有关其用户的大量信息。这些信息将通过传票和老式渠道提供给当局，在某种程度上也可供公众使用。

至少在美国，看看情报机构能拿到什么；

[image]

- 姓名
- 地址
- 服务年限
- 从开始到现在的所有服务（和帐户）的交易记录

以上只是至少，Twitter 可用的其他信息还包括：

- 物理位置
- IP地址
- 浏览器类型
- 引用域名
- 与广告的互动（收集更多数据）
- Cookies

甚至 **DM**！您认为私信的安全的？才不是，已经有发生的美国的案例显示，当局拿到了 **Twitter** 私信的信息，并以此作为证据缉拿目标人。这些信息将永久存储在Twitter，并可由法律机构随时收集。

必须知道，当局想要一切，所有历史数据，随时。 FBI 在处理 Tor 方面具有丰富的专业知识，能迅速处理已知的 Tor 出口节点；任何 VPN 都将以交换其信息为目标，这可能包括易于被识别的账单数据；在私有主机（例如 Algo 或 Streisand）上运行 VPN 之后将是来自服务器提供商的数据请求—再次，结算记录和用于创建帐户的 IP 地址将是最严重的威胁。下面是一个典型案例：

[image]

延伸：https://iyouport.substack.com/p/vpn?utm_source=publication-search

[image]

技巧的获得重在实践

和曾经推荐过的所有知识技巧一样，我们严重鼓励您去实践，因为单纯阅读是无法掌握它们的，知识不可能做到100%传播，大部分知识需要您通过实践自己总结，那些无法言说的部分价值会更大。

这些知识包括很多复杂的操作规则和指南，你必须严格遵守这些规范，如果不希望自己遭受危险的话。如果您能在实践中学习，您的错误将极大程度上减少。

所以，最好在非敏感帐户上执行这些规则，并保持这些规则，直到熟练地使用它们。确保你对结果感到满意，知道如何使用这些工具，了解你应该做什么以及为什么做。

应该知道，抵抗者前辈们有句俗语：第一个错误就是最后一个错误。因为你没有机会再来一次的，当你违反安全规则并导致被发现和曝光时。

你是抵抗者，你需要确保可以熟练使用安全工具并且不会出错——所以，先在安全的地方练习，将新手级的错误排除在外，然后在重要的地方安全地实施和操作。

[image]

如果您想要得到系统性的训练，或者您是培训师正在召集本地社区的入门级培训工作，建议从S01开始：[image]S01整体安全 - 总章节：前线安防入门课

破坏安全的对手

有许多主要对手很容易导致帐户用户的去匿名化。这些包括并不限于：

- 社交媒体

- 电子邮件/电话，链接到该帐户

- 执法者（或其他国家的国家权力）

- 新闻媒体/调查记者

- 同事/朋友/家人

显然，上述每一种安全对手的能力、意图和机会都不同，需要不同的技术来防止暴露，以保护自己。虽然面对如此大的侦查力量似乎令人生畏，但您的确可以有很大程度的自控能力。并且，其中大部分都并不费力，虽然长时间保持强大的安全状态需要专心致志。

—— 请记住，大部分时间里，专制政权都不会为追踪小鱼苗而烦恼。除非你已经被认为是“一个问题”，否则维稳经费不大可能“专门”花在你身上。但是你究竟是“大”还是“小”，我们无法判断，在不同国家有不同的判断方法，在中国，您需要咨询一些有经验的人。

但是，大多数时候，对你来说最大的威胁很可能只是因为你说得太多了，而且经常通过不靠谱的渠道说话，说得越多监视你的人就越了解你，越容易关注你，并找到你对当权者来说“存在危险”的证据。

对事物的恐惧比事物本身更糟糕，所以我们尽量不要强调它。我们要把重点放在安防习惯上，而不是加深你的恐惧。

心理健康风险

这也与安全有关？是的，而且关系很大！

一旦掌握并严格实施了技术保护和安全程序，您将面临的最大威胁就是您自己。

创建和维护一个秘密身份可能会很令人紧张，需要开发一种分隔的身份，一个残缺的自我，破碎的自我。从长远角度上看，这是有心理健康成本的，这就是为什么做间谍工作的人需要花费大量时间进行心理辅导—— 让心理学家为他们提供可以自由地谈论自己和自己关注的东西的唯一安全之所。

你有必要认真考虑一位专业的心理学家，在那里你将受到高度保密级的保护，你将能够自由地谈论你所承受的压力。

我们一直在考虑为异议人士提供这类专门的心理咨询服务，尤其是中国的异议人士已经普遍表现出虚无主义和焦虑症迹象的情况下。可惜目前为止都没有能让这一群体掌握基本安全通信知识和习惯，于是很难接触到他们。

[image]

[image]
[image]

袜子木偶 - 分身创建的小技巧

[image] 关键词	个人 免追踪 分身 反侦察 反间谍 数字足迹 自助 预防性
[image] 关联	[image]简易分身术：妥善管理您的在线身份并获得安全的方法
[image] 创建时间	2019年7月12日
[image] **Description**	操作安全性

可能您有很多理由需要在网上有意识地创建一个或多个、虚假的、匿名的或假名的身份，尤其是作为正义的目标，它很重要。我们来详细说说这事大致应该怎么做……

- Table of Contents

  起步 - 设定形象
  - 不要使用名称或物理描述来启动这一伪装角色。
  – 如果可能的话首先探索一下。
  – 给自己设置一些问题。
  – 与你的角色感同身受，但不是同情。
  – 花时间进行实验。
  给你的角色一个故事
  细化品格——
  – 创建角色的名称和外观。
  – 为（每个）角色建立个人资料。
  – 添加一些情感。
  – 定期重新访问您为角色制定的配置文件和方案，以进一步调整和细化。
  讲故事和作者识别——
  合理否认——
  下面总结并补充一下：创造一个可靠的角色
  语言指纹——
  工作——

技能和兴趣——
心理态度——
创建在线资料——
关于语言学取证，另外推荐一些资料，包括两个纪录片

[image]

你不是 troll 我知道，但是人们可能有很多理由需要在网上有意识地创建多个、虚假的、匿名的或假名的身份，尤其是作为正义的目标，它很重要。

比如：

- 参与当下的行动、而避免过去或将来的信息被用来作为参照。比如你声援一位敏感人士，或者你准备发布一些紧要的机密信息；
- 采取新身份成为一个自然而然的人，无拘无束地发表言论。这应该非常参见；
- 游戏、爱好、（在线）角色扮演、与 trolls 展开战斗、防御大规模监视、为监视制造混乱等等，你可以大胆行事，化身不会自动成为你的真实身份的一部分；
- 仅仅希望在线生活更具弹性；
- 通过分离专业和私人信息，提高个性、自主性和自由度；
- 挑战自我，抓住优势；
- 内容营销和自我权威……

可能很多人会觉得自己很擅长伪装，我承认这的确是部分人的天赋，

但不一定所有人都了解该如何彻底切断与真实身份的联系，包括那些自认为擅长者。今天来大致说说这件事。伪装术亦正亦邪，其性质完全取决于您的目的。

本指南仅讲述在线伪装。关于现实中的伪装术详见 [image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 。

下面我们开始。

起步 - 设定形象

注意事项如下：

- 不要使用名称或物理描述来启动这一伪装角色。

因为我们所有人都有很多关于名字和体型的先入为主的想法。

如果你从一个名字或外表切入，这个角色就会自动携带很多你自己甚至可能都不知道存在的信息。

比如，首先映入你脑海的字样，它就存在于你的个人经验和性格中，也许你没有发现它和自己的关系，但是对于挖掘你真实身份的人来说，这就是一个有效的线索。

[image]

扮演游戏中你的原则应该是：彻底切断伪装身份和真实身份之间的联系。

随时谨记这一原则。

– 如果可能的话首先探索一下。

如果你有时间，可以试着适应一下角色所处的环境，以便正式运行时你可以自如发挥而不会出格。

每个上下文都有自己的“味道”，并且有趣的部分是要知道在特定（一组）上下文中什么是不可能的、什么是可能的。上下文也可以成为挑选角色的灵感来源。

总之，你的角色是“一个真实的人”，它应该血肉丰满合乎逻辑。

– 给自己设置一些问题。

用戏剧性的需求和强迫来培养你的角色品格。

这个角色想要什么？要避免什么？问问自己，你想对这个角色做些什么。

例如，如果你要引导这个角色进入大众视野，你的能量必须与你将要扮演的角色相匹配。如果你的个性或心理构成特点无法让你轻松发挥某些特定的作用，那么就不要尝试，避免出错。

– 与你的角色感同身受，但不是同情。

将角色扮演设置为你熟悉的事，当你扮演的是恶棍时，你必须成为那个恶棍。

你必须明白恶棍的行为和思考方式。这些时刻的感同身受可能是一种痛苦，但你不能让感同身受变成同情并诱惑自己让恶棍脱离情境。

审视自己人性中的黑暗面，以提供一个可信的邪恶角色。

这只是举一个比较极端的例子，比如当你想深入敌人内部的时候，这种方法用得到。只有当他们把你当成自己人时，你才有希望达成目的。

– 花时间进行实验。

也就是我们一直强调的，多练习，直到融为一体。

给你的角色一个故事

越来越多的心理学家认为，生活在现代社会中的人们通过构建和内化自我定义的故事来赋予生活的意义。无论如何，“用故事讲述身份”的做法对我来说似乎很过时了，相反，采取一个带故事的新化身会使维护这个角色变得容易得多。

你可以编造自己的故事，使用“已知”人物的故事，或添加其他故事情节（将故事放在另一个背景中，而不是故事起源的地方）都会非常有趣，一个像匿名者那样的“群体身份”，但并不是一个传统的有形的组织，等等。

故事的目的是在任何时候任何对话中你的角色都能自然而然并符合逻辑地自圆其说。

角色就是一个人，它虽然与你毫无关系，但你必须变成它，才能自如地控制它。

细化品格——

– 创建角色的名称和外观。

所有一切信息都需要协调，这非常重要。

没错，在现实中的确存在身份信息不同方面存在不协调的真实的个人，但是角色扮演不能这样做，以避免引人注意。

你的主旨应该是融入，而不是出众。

– 为（每个）角色建立个人资料。

关注在角色开发阶段中你可以找到的任何缺失元素，补充完整。

– 添加一些情感。

情绪远远超出/微笑/调情和/害羞，它应该更加丰满，并且随时注意要贴近您希望该角色表达的主题。

– 定期重新访问您为角色制定的配置文件和方案，以进一步调整和细化。

调整一定要以整体逻辑不变为宗旨。

讲故事和作者识别——

随着互联网让我们之间的沟通变得越来越多，我们每个人留下的语言指纹也为调查人员提供了诱人的线索，为语言学取证的小而有影响力和不断增长的领域做出了贡献，并为其有争议的子专业—— 即 作者识别，做出了贡献。

[image]

激进社区用户请从这里进入：[image]语言指纹

要查看您留下的一些语言指纹，您可以使用 Java 图形作者归因程序，这是一个方便的应用程序，可用于文本分析和作者归属。作为基于 Java 的模块化程序，它可以在任何安装了 Java 版本的计算机上运行。

在作者或博主的词汇表中提取一百个最常用的单词。此步骤消除了罕见的单词、字符名称和情节点，连接词似乎没什么特别的，但是它的使用数量和频率是一个很强的参考值，它们可以在任何一个词上留下作者的“指纹”。

无论你发现了什么都只是线索，而不是无可辩驳的证据。取证语言学的起源可能很古老，但这种分析目前正再次兴起。限制因素一直是时间和精力，但随着电子书和博客随时可用，几乎可以针对任何作者快速分析。

这对于那些寻求化名以实现言论自由的作者和博主来说简直太糟糕了，除非使用某些替换方案（配置你的自动更正应用程序）作为创建可靠角色的一部分。这可能还不够，取决于具体情况。

Chaski 认为关键不在于扫描文本—— 无论是通过眼睛还是机器——这只适用于肤浅的特质，而是用于表达句法结构的语言学家研究。她没有透露她的方法是如何运作的，但她表示已经通过“组成结构”的分析模式达到了约 95% 的准确率，通常是人们下意识在一个句子中组合短语的习惯。

她解释说，有些人会产生复杂的名词短语和简单的动词短语；其他人会产生复杂的状语短语，等等。通过不仅关注词性，而且关注如何使用这些词性，她的分析似乎摆脱了对词语和拼写的依赖。

如果我们的语言确实与我们的 DNA 一样独特，只能说我们还没有解码它。很快就会有人因基于他们的文字中找到的线索而被定罪吗？这是一个很大的问号，就像调查取证和法庭中已经被接受和广泛使用的一些生物识别技术一样。

合理否认——

“合理的否认”是指受试者可以安全和可信地否认可能存在的任何特定事实的情况，因为该受试者故意不知道所述的真相，从而使受试者从任何责任中受益或受到保护。这是它的基本定义。

为您的角色添加合理的否认模式可能会很有用，因为监视系统可以关联所有类型的信息、但却无法解释非信息，贝叶斯逻辑也不能处理角色扮演与无知之间的差异。这个问题更多关于“混淆监视系统”，可参见关于 Non-classical logic 的分析资料。

网络：以某种方式自动转发某些类型的广播，使得文件的原始发送者与仅仅转发它的人无法区分，允许首先发送文件的人声称只是转发者，并且如果没有与该人的计算机之间的所有网络连接的完整解密日志，则无法证明此声明。freenet 文件共享网络和审查解决方案，例如通过模糊数据源和流来保护运营商和网络用户，防止审查者知道数据来自何处以及存储在何处。

可否认的磁盘加密：使用隐写术，其中加密文件或消息的存在是可否认的，因为攻击者无法证明存在加密消息。

[image]

可在本站“工具”专题中搜索“隐写”，以找到相关工具。

下面总结并补充一下：创造一个可靠的角色

虚拟角色或身份不能只是具有邮件地址和一系列 Web 帐户的名称。如果我们保留所有正常的识别特征—— 例如性别、工作、态度或我们写作的方式—— 那么有人就可能找到关联点并将我们创造的假人物与我们的真实身份联系起来。

语言指纹——

要考虑的第一件事是语言指纹。这是可识别的，文本分析识别工具正在越来越多地被使用，即使对于非专家来说也是如此，这使得可以识别特定文本的作者。

例如，可以通过我们写出的某些单词、典型的错别字、以及我们的风格和语调的特定方式来识别真实身份。要避免它，可以先在字处理程序中使用拼写检查器来检查是否存在一致的拼写错误；也可以考虑采用不同的写作态度。

为了简单起见，可以为每个角色采用一套简单的规则，例如，只使用大写字母的怒目圆睁风格，或者是只使用小写字母的低语者风格，或者表现非常兴奋、带有很多感叹号，或者故意拼写错误、总是将撇放在错误的地方等。

工作——

为了确保假身份无法追溯到我们的真人，被创造角色应该有一份与我们不同的工作，但你不能对该领域一无所知：例如，不应该在对解剖学一无所知的情况下假扮外科医生。

技能和兴趣——

应该类似的考虑选择角色的技能和他们关注和写下的主要话题。当然，这些可以重叠，例如，撰写国家政治的记者可能有另一种身份，谈论国家政治，但只是随便说说而已（他们的主要兴趣将是不同的东西，如木工或女权主义或美食）。

心理态度——

至于心理态度，一个好的经验法则是通过创造一些“弱点”来给予我们的角色以人格深度，但要仔细选择它们，这样，如果弱点受到攻击，我们就能够抵御，甚至在这个过程中获得一些乐趣。例如，如果你有

一种非常强烈的幽默感，就可以选择严重缺乏幽默作为角色的最大弱点，这样如果这种弱点受到攻击，就可以享受冒充幽默的角色而不会真正受到心理伤害。

最重要的是要记住，在互联网上，我们的每一个身份—— 甚至是与我们的真实姓名相关的身份—— 都是一个“虚拟”身份，而且最好决定你想要在每个身份中暴露哪些性格特征。即使对于我们的“真实”在线身份创建一个有点虚构的角色，也是一个好主意。

创建在线资料——

一旦创建了几个角色，重要的是让它们在我们的物理和数字生活中切分开。虽然记录我们的身份可能有助于确保自己记住设定的故事，但也可以采取技术措施来确保个人资料保持独立。

[image]

一个好的开始是为每个身份创建不同的浏览器配置文件、邮箱和社交网络帐户。一个好的经验法则是：始终为每个帐户/身份使用不同的应用程序，如果可能的话，将每个设备或操作系统区分为不同的身份。

创建新邮箱时，最好使用 Torbrowser 连接，如果需要联系电子邮件地址，请考虑使用一次性电子邮件地址。

- 一次性电子邮件地址

对于某些活动和社交领域，我们需要管理一个圆润的角色，以获得社区其他成员的良好声誉和信任。但是，在某些情况下，所需要的只是一次性电子邮件地址，只需要使用一次或几次，例如在不受信任的平台上开设帐户。

即使你决定在线只有一个身份，使用一次性电子邮件地址也可以防止网站建立关于我们活动的历史记录，并确保如果该帐户遭到入侵，可以简单地删除它并创建一个新的，保持数字生活完好无损。

有许多服务提供一次性电子邮件地址。比如：https：//anonbox.net，由混沌计算机俱乐部提供，和 https://www.guerrillamail.com

[image]

可在本站“工具”专题中搜索“电邮/电子邮件”，以找到相关工具。

- 生成个人详细信息的工具

Fakena.me是一个面向隐私保护的“虚假名称生成器”，可以为您提供一切可靠的名称、出生日期和（美国）地址、用户名和密码以及指向已连接的邮箱的链接。另一个名为 Instant Internet Decoy（https://decoys.me）的类似服务也创造了令人信服但完全虚构的人，他们的生日、在多个国家/地区的家庭、甚至回答常见的安全问题。

还可以使用现有的虚假或一次性电子邮件帐户。BugMeNot（http://bugmenot.com）允许人们分享他们为免费注册平台创建的电子邮件登录名和密码，供任何人使用。

另一种选择是创建邮件别名—连接到你的主邮箱的其他电子邮件地址。这种方法的优点是该电子邮件帐户不会过期，如果它被泄露，那就处理它并创建一个新的。但当然，如果别名收到大量垃圾邮件，它将填满你的主邮箱。

虽然并非每个邮件服务都允许用户创建邮件别名，但此服务提供给 Riseup（https://we.riseup.net）和 Autistici / Inventati（https://www.autistici.org）的每个邮件用户，这两个都值得推荐，特别关注隐私权和匿名权。

关于语言学取证，另外推荐一些资料，包括两个纪录片

The meta book and size-dependent properties of written language http://arxiv.org/abs/0909.4385 (2009)

On Linguistic Fingerprinting http://thelousylinguist.blogspot.nl/2009/12/on-linguistic-fingerprinting.html (2009)

Empirical evaluations of language-based author identification techniques http://nlp.cs.swarthmore.edu/~richardw/papers/chaski2001-empirical.pdf

The role of forensic linguistics in crime investigation http://www.academia.edu/3573524/The_Role_of_Forensic_Linguistics_in_Crime_Investigation (2012)

Syntactic Stylometry: Using Sentence Structure for Authorship Attribution http://www.ai.uga.edu/sites/default/files/theses/hollingsworth_charles_d_201208_ms.pdf

Linguistic Hacking [24c3]

Automatic Sentiment Detection in Terry Pratchett's Discworld @ ELC3—Santiago de Compostela, Spain

[image]
[image]

移除你的绵羊墙：给普通人的5个防御课程

[image] 关键词	个人 数字安全 防御
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2019年7月24日
[image] **Description**	操作安全性；技术直觉

学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。

- Table of Contents

第一课：批判性思维
攻击者是如何绕过防御的 ——
第二课：学会悬停
万一不小心点击了链接后才感觉到危险怎么办？
如果事发时你联系不到任何人，该怎么办？
攻击者是如何绕过防御的
第三课：URL解析
攻击者是如何绕过防御的
第四课：分析邮件头
攻击者是如何绕过防御的
第五课：沙盒
攻击者是如何绕过防御的
坏主意陷阱：移除你的绵羊墙
1、“复制粘贴，解决麻烦”
2、“分享也是关照”
3、“好的反病毒软件能拯救你”
总结

下面是阅读本文后您应该知道的：

[image]

就如您所知道的，安全不是一个人能独自完成的工作。确保您的周边朋友/社区/团队/组织中所有人都具备足够的安全意识和防护能力，您才能做到安全。

于是基础知识培训是重要的。我们知道很多人在询问相关知识，并且很积极地向自己周围的朋友推荐，这非常好；敏感人士社区和组织内部也做了一些安全知识辅导。但我们发现，其中有一些安全培训是不充分的甚至其建议是不恰当的，有可能起到反作用。

此外，培训和介绍知识也不完全相同，培训需要的技巧更多，尤其是，培训的主旨应该在于培养洞察力、机动性和创造力，而非死记硬背。在安全方面这至关重要。

本文将基本层面上做一个简单梳理，介绍五个基础的培训课程，并介绍一些较为常见的错误建议。如果您还有遇到过其他错误建议，或者您在培训方面有更多经验，欢迎留言讨论。

关于社交工程攻击和钓鱼的基本知识可参见本站 🍎 心理安全-PsychologicalSecurity ，这是关于人们是如何中招的、攻击者是如何思考的、技术社区如何协助活动家增强安防……等等，现在是时候进行自我保护了。如果您还没能获得技术专家的协助，自己也可以完成基本部分。

本文更多是给普通人的。如果您身边没有专业全职的技术人员可以随叫随到，本文会适合您，不论您从事什么职业、持有什么政治观点、是否属于少数族裔或边缘群体，等等，都无所谓，只要您还在使用互联网，这些知识就是必需掌握的，否则就会变成众矢之的。

本文还会有一面绵羊墙。 wall of sheep - 如果您不是技术人士可能对这个词还不太熟悉，它来自于 DEF CON，全球最大的黑客会议之一。在每年的 DEF CON 上，运作绵羊墙的人都会把在会场上连接到

未知网络的“绵羊”们的账号密码公布在上面。为什么要这样做？他们希望能借此提高人们的安全意识，告诉人们抓取这些信息有多么容易。

下面分别介绍5个防御课程。

[image]

第一课：批判性思维

- 类别：普通和专业

很多时候人们会把批判性思维和逆反、缺乏信仰或者为了质疑而质疑，混淆在一起，但这不是批判性思维真正的定义。

在本文的主题里，批判性思维指的是：告诫自己不要事事都信以为真；不要以为没时间评估、压力太大来不及思考就将信息理解为真实。只需要稍稍停下来想一下，就能避免杏仁核劫持发生的决策错误。问自己下面这些问题：

- 这封邮件/短信/留言真的来自我认识的人吗？

- 我预料到会收获这样一条信息吗？

- 信息中含带的请求合理吗？符合我认识的那个人的性格习惯吗？

- 这条消息是否在试图唤起某种情绪，比如恐惧、贪婪、强大的好奇心，或者最重要的 —— 它是否试图让我做点什么？

只需要两三秒钟想想上面这些问题，就能帮你更好地识别钓鱼攻击。将上述问题运用到下面的课程中，并且您会发现，在识别真正的威胁时，思考和不思考上述问题的区别是很大的。

攻击者是如何绕过防御的 ——

攻击者不希望你思考，尤其不希望你进行批判性思考。他们会利用情绪阻止你进行批判性思考，唤起你的恐惧、忧伤、愤怒，迫使你采取不该采取的行动。这是社交工程的一个最基本的模式；民粹政客使用的也是这样的模式。

防御办法很简单，停下来几秒钟就可以做到，先放下它去读点别的东西，你的杏仁核就又属于你了。

第二课：学会悬停

- 类别：普通和专业

想象你坐在家里或办公室里，然后收到下面这样的邮件，你会是什么样的感觉？

[image]

你可能会开始想："不能让我的UPS包裹出问题，最好检查一下"。或者，你并没有UPS账号，但也会惊慌："谁用我的名字建立了一个UPS账户？"

还记得著名流亡异议人士奥马尔·阿卜杜拉齐兹是如何被间谍软件攻击以至于害死了他最好的朋友华盛顿邮报专栏作家贾迈勒·卡舒吉吗？

[image]

延伸：https://iyouport.substack.com/p/4bc?utm_source=publication-search

不管是上述哪种情况，恐惧和好奇都会促使你去点击那个链接。这封邮件有正确的标识，看起来很正式，甚至可能和你收到的任何USP邮

件都十分相似。这些细节使得你相信这是一封真实的邮件。

但这的确有可能是一个精心设计的恶意钓鱼邮件，目的是让你下载恶意软件、泄露信息、悄悄控制你的设备。

你需要做的只是把鼠标悬停在链接上，只是悬停就可以，不要点击！看看会发生什么，类似于这样：

[image]

具体到人的情况也许不同，但是如果你在美国，你就会产生怀疑："为什么USP会把我的账户信息存在一个南美的服务器里？"——后缀".za"表明了这一点。

因为悬停就可以反应出URL地址，而这个地址并不像USP，所以这是钓鱼邮件。现在看内容。

这封邮件的意思很含糊，你甚至都无法如实回答第一个问题；你没有期望或请求这封邮件，而URL指向一个完全不同的网站。那就马上删除它。

但请记住，有些情况下，高明的攻击者可以阻止悬停，所以，当你点击前务必要再次确定地址栏中的地址，以确保你访问的是一个合法地址。

虚拟机是再好不过的了，隔离危险的最佳选项，不过这只能防止一般性的攻击。后面有更多介绍。

[image]

延伸：https://iyouport.substack.com/p/--62e?utm_source=publication-search

万一不小心点击了链接后才感觉到危险怎么办？

不幸的是这种情况的确会发生。如果你是公司员工，可以反应给技术部门，能节省很多时间；如果你是私人、孤军奋战的活动家，有一些求助渠道可以参考：

[image]

返回：[image]设备好像被黑了怎么办？ - 数字急救包

如果事发时你联系不到任何人，该怎么办？

别慌。首先，回想一下当你点击链接后网站向你发出了什么请求 —— 你被要提供账户信息吗？被要求输入账户名密码？或者被要求下载一个文件、安装一个程序？

如果你输入了账户名密码，那就要立刻确认是否在其他地方也使用了相同的账户名密码；找到同样的部分，立刻修改它们。

如果邮件中提到了某个公司的账户，而且你输入了网站，那么就给那家公司打电话，告诉他们你可能把你的账户信息告诉了某个恶意组织，让公司修改你的账户信息以保护你的安全。

如果安装了那封邮件中要求你安装的程序，就要立刻清理电脑，并在另一台安全的设备上修改绝大多数账户名和密码。

我不可能知道你中了哪种病毒，所以无法说明接下来应该做什么；如果你也不知道该如何处理病毒，所在社区也没有专业技术服务和联盟的话，就联系这篇文章中提到的组织。

不要惊慌，但并非不要紧张；要尽快采取行动才行；而惊慌会让事情变得更糟。深呼吸，回想一切可以止损的方法。

[image]

特别建议从这里进入相关议题：[image]数字技术限制和最佳实践

攻击者是如何绕过防御的

攻击者会意识到潜在的受害者受过一些训练，比如知道如何悬停以验证等等；很多邮件服务也会检查URL是否和文本中显示的不同。攻击者可能会购买非常相近的域名来掩饰他们用来攻击的真实域名。

比如这样 ＜secure-你的银行.com＞ 域名，而你在这个链接上悬停，你会看到“正确“的域名，也许就会信以为真。这个时候批判性思考就要起作用了：想想看你的银行是从这个域名给你发邮件的吗？如果有所怀疑，那就要检查一下。

其他攻击者会用注册过的证书来使得网站看起来合法和安全，并且攻击者确实拥有这些证书。这些证书可能会以狡猾的方式命名，比如trusted、secure 等等，让你以为它是安全的。

另外，攻击者会攻击全球范围内真实的服务器，并用合法服务器发送钓鱼邮件。通常攻击者会获取这些设备上的邮件地址，然后利用这些邮件地址来联系第一批受害人。

所以，始终记得要点击前三思 ＋ 虚拟机 ＋ 谨慎输入信息。

[image]

第三课：URL解析

- 分类：普通和专业

本节不是写给专业人士的，如果您有技术基础，那就跳过它。

URL有几个组成部分：协议、子域名、域名、顶级域名、文件地址、资源。

为什么理解URL很重要？因为很多钓鱼攻击就是在利用认识不足来欺骗你的。比如，我声称来自微软，并希望你下载一个名为 file.txt 的文件，那么你能识别下面这些网址中哪些属于微软，哪些是潜在的威胁吗？

- http:// microsoft. com/ file. txt
- http:// secure-microsoft. com/ file. txt
- https:// secure. microsoft. com/ file. txt
- http:// microsoft. com/ secure/ file. txt
- http:// rnicrosoft. com/ file. txt

第一个网址是合法的，虽然缺少了www，但它确实指向真实的微软网址。

要小心对付第二个，它可能不属于微软，secure-microsoft 中的“-” 表示它和微软域名完全不同。

第三个是安全的。它属于合法公司，而且位于https。secure 子域名隶属于微软的域名。而第二个网址则试图伪装成一个安全网址，但实际上使用了“-”而不是“.”来分割地址。“.”意味着该子域名属于主域名，而“-”指向一个全新的域名，因此第二个网址是不可信的。

第四个网址也是合法的，只是位于下一级域名。

第五个很有迷惑性，那不是 **m** 而是 **rn**，如果靠得足够紧，一马虎就容易看错。这类东西特别多，比如大写的“I”和数字“1”的混淆，等等。

当然，恶意攻击者还有很多诱使受害者点击链接的手段，这也是为什

么学习URL很重要。即使是有经验的安全专家也有可能犯错，但是相关培训肯定能帮您和您的团队/组织减少风险。

攻击者是如何绕过防御的

和前面描述的悬停一样的，攻击者可以购买一些看起来合法的域名。这些域名与真实域名越是相近，你就越容易相信它是真的。

再次强调，secure-DOMAIN.com 是一个完全不同于 DOMAIN.com 的新域名，但如果它是一个合法的名称结尾，很多人会误以为它是合法网址。

同样，攻击者会攻击全球服务器，然后利用这些合法服务器来发送钓鱼邮件。这类攻击是非常危险的，也很难检测。

再一次，运用批判性思维，点击前停下来想一想，问自己一些分析性问题，都可以帮你从容应对。

[image]

第四课：分析邮件头

- 分类：专业

由于有大量的邮件服务商存在，我无法告诉你如何定位每一家服务商的邮件头，但我可以告诉你它们是什么，以及你可以如何利用它们。

在选定的搜索引擎中输入 Email headers in ＜服务商名称＞来弄清楚自己的服务商的邮件头。

这就像是GPS。你来到我家，我可以查看你的行程历史记录来确定你走的是哪条路线。如果你告诉我你走的是第一条路线，但是GPS显示

你花了大量时间在第二条路线上，那么我就知道你迷路了。

邮件头与此类次，它们可以告知你邮件是如何到达你的邮箱的。看下面这个例子。这封邮件声称来自达美航空公司（Delta Airlines），并说收件人的航空里程账户有异常情况。

[image]

如何你感到困惑，请尝试拆分邮件头，如下表所示，这样能看得清楚一些：

[image]

SPF是 Sender Policy Framework（发送方策略框架），是一种以 IP 地址认证电子邮件发件人身份的技术，被用来识别垃圾邮件；“退订信息”是指服务器提供给用户用来快速退订邮件的按钮的字段。

可以清楚看到这封邮件被发往了正确的地址，回信地址和回复人都清楚地指向了 delta.com 我们也可以在域名签名和信息ID上看到 delta.com。这表明邮件是来自它所声称的合法地址，也意味着它是可信的。

如果检查邮件头中的域名和邮件中的域名毫不相干；回信地址和认证结果也与其声称的无关，那么就可以肯定不受信任。

攻击者是如何绕过防御的

检查邮件头就可以确保安全吗？不会。有些钓鱼邮件攻击附带一个目的：对网络进行渗透，然后获取使用 **SMTP** 服务器的权限。为什么要这样做？

你曾经收到过来自自己朋友的邮件，却发现是一封非法邮件吗？这种情况可能已经不罕见了，而且短信也可以做到篡改发信人。

毫无疑问朋友是最容易对我们形成影响的人，攻击者当然非常清楚这个道理，让你信任一封邮件中的附件、链接或者文件，没有比伪装成

你的朋友更好的办法了。

攻击者会使用任何方法获得你朋友的设备的访问权限，用所有好友和收件箱中的联系人随机分发恶意邮件。这种时候检查邮件头是没用的。

再一次，批判性思考非常必要，并且，你需要 对自己的朋友（那个发件人真身）有足够的了解 ，尤其是，你 应该和注重安全也懂安全技巧的人交朋友 。否则，一个*疏忽大意的人就有可能会害了你们关系网中的一大群人。

[image]

第五课：沙盒

- 分类：专业

沙盒就是指创建一个可以运行未经测试或者不受信任的代码的环境，这些代码可以包括病毒和恶意软件。用户想要在自己的系统或网络中使用它们之前，可以拥有的一个几乎对主机没有任何影响的环境，在这里测试这些代码。

这个概念非常简单，就像下面这样：

[image]

这是最简单的方法。您无需懂技术也能在理论上轻松避免被攻击。但是这并不代表万无一失！

沙盒是技术问题，单纯的技术无法解决基于人性弱点的社交工程攻击。

攻击者是如何绕过防御的

曾经有一个这样的案例，关于附件中附带某种来源于一个叫 Quarian 的组织的恶意软件，这种恶意软件能伪装成PDF、DOC或者XLS文件，而且此后该恶意软件还升级了，新版本包含了一些需要被注意的功能：

- 它自动安装称成一个 Windows 服务，不再只是一个运行程序；
- 它通过运行一系列命令连接到国外服务器下载有效荷载；
- 尤其是，它依赖 **AppleID** 或者命令行交互，因此它不会被沙盒检测到。

并且不止这些。通过虚拟机直接感染主机的恶意软件也不是没有。（所以，显然 Whonix 的思路是更好的，即便恶意软件穿透了一个虚拟机，它也透不过第二个）。

没错，攻击者一直在变得更加聪明，因为他们整天琢磨这些事；安全防御技术需要不断更新才能跟上这一进度。作为培训师你应该首先和你的服务对象讲清楚 —— 昨天提供的方案今天失效了并不意味着昨天在骗人、更不意味着安全防御是令人焦虑的和无用的，正相反，这只是在提醒人们持续保持警惕的必要性，学习不是几堂课的任务。

谨记一条规则：仅仅依靠技术并不能让你免于社交工程攻击。

[image]

[image]

坏主意陷阱：移除你的绵羊墙

鉴于威胁的无处不在，人们一直在纷纷想办法解决问题，不断向自己所属的组织、社区和合作团队推荐方法。其中有一些甚至有希望成功，但是，应该被归为“坏主意”。

下面是一些曾经被很多使用过的坏主意，分析下他们为什么弊大于利。

1、“复制粘贴，解决麻烦”

这甚至很可能是来自一场正规的安全培训中传授的方法；当时讲师表示：“如果你不确定你接收到的链接是否安全，那么复制粘贴到浏览器的地址栏中”……

其实这是史上最糟糕的建议。如果你收到一封钓鱼邮件，里面附有一个链接 www. superbadhackingsitethatwillruinyourlife. com，你选中它，然后复制、粘贴，那么你猜你会进入哪个页面？没错 —— 你仍然访问的是 www. superbadhackingsitethatwillruinyourlife. com。

你也许会说，如果URL看起来像是 www.microsoft.com 而它指向的是一个恶意网站，那么复制粘贴不就会失效了吗？

是的，技术上来说，如果你让你的用户只是复制那段文本，那么他们将会访问的就是那个文本所示的网站。但是如果用户误点了那个链接而不是复制，或者错误的选择了右键复制而不是选中复制，或者两者全做了，他们仍然会访问一个恶意网站，并且可能直接被感染。

所以，培训师应该告诉用户：不要碰那个链接，离它远一点；除非你非常熟悉如何解码**URL**，否则不要试着分析它。

2、“分享也是关照”

另外一个馊主意是这样的：“我刚收到了一封钓鱼邮件，我认为可能是钓鱼邮件，我把它转发给最懂电脑的五个朋友，这样他们就能告诉我这是不是钓鱼邮件了”……

如果你这么做了，其结果就是：你把一个带有潜在危险的恶意邮件转发给了五个人。如果这些朋友和你在同一家公司/同一个组织工作，那么你就是在该组织/公司内部扩散了潜在威胁；如果这些朋友在其他公司/组织工作，那么你的做法就是在传播病毒，是在帮助社交工程攻击者完成目标。

或者更形象一些，换个说法："如果我怀疑自己感冒了，那就找五个朋友去他们面前咳嗽，如果他们也感冒了，那么我就可以确定我感冒了"。

有一个渗透测试是这样的，USB密钥遗失测试。在USB密钥中放置一个PDF文件，这个文件的功能是"给家里打电话"。它连接到测试者服务器后会连接到一个 Metasploit4，并给测试者一个远程shell。这个PDF文件被命名为"员工奖金" EmployeeBonuses。

测试者将这个USB放置在预先约定好的地方。等他们返回办公室的时候已经有7个shell的。这7个shell来自人事部门、IT部门、以及同一个部门的其他地方。很惊人吧。究竟发生了什么？

其实很简单。第一个人试着打开 EmployeeBonuses.PDF 文件时文件崩溃了。于是他就拿着这个USB去了人事部门，找一位更高明的朋友帮忙；当然，在第二个人那里也崩溃了，于是他俩就跑去IT部门找人帮忙。IT部门在第三台电脑上试着打开它……

这些人在试图打开一个文件，看看他们的奖金发生了什么，就这么一个简单的过程结果是把这个东西传到了整个公司。

在这种情况下，分享并非是一种"关照"，而是伤害。可疑的钓鱼邮件尤其如此。

3、"好的反病毒软件能拯救你"

反病毒软件是为阻止病毒的。病毒有自己的签名 —— 这是病毒内存在的一系列指纹作用的代码。就像你我的指纹可以用来识别身份那

样，病毒的指纹也可以用来识别病毒。

这些病毒的指纹被放进了反病毒软件的数据库中，然后反病毒软件就可以对你的电脑进行扫描；如果发现了某个网页、文件、文件夹或者程序有这些指纹，就会清除它，以确保它不做进一步破坏。

听起来很棒。但是，反病毒软件是管理软件，而不是安全软件。反病毒软件可以帮你识别出已知签名的病毒；但是如果病毒是新的，还没有登记指纹呢？如果病毒使用多态 shellcode 呢？（shellcode 会在每次载入时改变自己的签名）根本无法检测对吧？

这是否意味着反病毒软件根本没用，不需要购买安装了？并不是。你应该继续使用好的反病毒软件，它们可以抓住那些已经流行了一阵子的病毒；但是你不应该把它当成救世主，它无法帮你抵御特别有目的的攻击者。

总结

说到 shellcode 想起一个编码工具：一个人们可以通过对 shellcode 进行编码来给它一个全新签名的小工具 —— Shikata Ga Nai。这是一个多态编码工具，名字来源于日文，意思是“无事可做”，或“没有希望”。本文的内容并不是让你感觉“shikata ga nai”，正相反是为了找到一些希望。

下面是阅读本文后您应该知道的：

- 坏人更高明、更加坚定和努力。他们似乎一直领先于你，并依靠你的弱点获胜；
- 仅仅依靠技术是救不了你的，技术也不应该被视为社交工程攻击的唯一解决方案；

- 钓鱼攻击是真正的威胁，也是最经常出现的和最容易得逞的威胁；

- 如果你的工作是确保组织和团队的安全，那就找到那些给你出坏主意的人，清除那些坏主意。

[image]

教育是解决问题的关键。必须和你所在组织团队/社交圈子一起努力，进行持久的、定期的、基于真实案例的教育，让你的周边人形成一种安全文化意识，否则一两个人的努力是不会让你获得安全的。

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

你可能会说你试过所有这些方法，但是“周围人对此不感兴趣”。没错，我们在中国的活动家、记者和人权维护者群体中也看到了同样的状况。理论上我们认为这些敏感人士应该是最注重安全保护的人群，而事实上并非如此，人们对安全知识表现淡漠。为什么呢？

因为这需要技术社区做好渗透测试服务，以及组织团队的管理者与技术社区的紧密合作。社会工作一直比技术工作更复杂，需要很多技巧。

我们一直在撰写各种保护知识和技巧的文章，向敏感人群解释加密的消息服务、安全电子邮件的重要性、社交工程学的攻防技巧、如何保护社交媒体的帐户和宣传能力等等，这些都是必不可少的。但事实却是，有关如何使用 Signal 、保护数字隐私的大量指南、以及诸如“使用 Tor”的多项须知等等广泛声明，可能难以被非技术人士理解，更不用说采取行动了。这就形成了一个根本性的错位。

与此同时，慈善组织也很难了解究竟什么样的技术专家才是活动家、边缘社区、记者和人权维护者最需要的。

这些差距显而易见。但是没有人应该为这个差距负责。现有的数字安

全资源通常是旨在帮助个人确保他们的数字足迹避免被识别所需的工具，或者在发生紧急情况和关键威胁时做出的响应。教授整个组织及其资助者 —— 如何深入了解数字态度和习惯，如何分析敏感用户、组织和以任务为中心的数据使用、保留和共享，将更加困难。

[image]

我们要的并不是亲自动手帮助敏感人士安装一个 **Whonix** 就完工了，而是最终能让人们知道遇到紧急状况时应该怎么办，尤其是如何形成结盟网络，让求助变得更容易。也就是，形成能够让自己变得更强大的思考方式。

这就是为什么在这个对民间社会数字基础设施的攻击日益复杂的时代，我们需要支持在组织层面进行更大的能力建设。

[image]
[image]

简易分身术：妥善管理您的在线身份并获得安全的方法

[image] 关键词	分身 反侦察 反追踪 数字足迹 自卫 预防性
[image] 关联	分身
[image] 创建时间	2019年7月26日
[image] Description	操作安全性

对于所有人，只要您在互联网上，而不仅仅是敏感人士 - - 关于什么是数据？什么是数字阴影？如何避免被追踪迫害？如何变成另一个人？尤其是如何分裂为多个不同的人？

- Table of Contents

  数字阴影都是什么？
  谁在收集我们的数据，为什么？
  探索你自己的数字阴影
  控制您共享的内容和元数据
  社交领域
  自我人肉
  删除你的过去，创建新身份
  以下是当你开始做这件事时的基本注意事项：
  删除身份
  映射你的社交域
  评估风险和潜力：如何选择适合我们目的的在线身份
  “真实”还是虚拟身份？
  在线分离身份的策略
  匿名——
  持久的假名——
  集体身份——

比较策略——
创建新的在线身份
1、起个名字
2、写自己的故事
3、创建在线资料
4、创建单独的浏览器配置文件和邮箱
5、在社交网络上管理身份
6、另类社交网络
7、创建博客或网站
管理集体在线身份
1、集体虚拟角色
2、管理集体身份......或简单的集体账户
每个身份的不同设备——
Tails——
隔离安全性：Qubes OS——
那么 Tails，Whonix，Qubes OS：应该如何选择

[image]

互联网是探索、学习、说话、倾听和与世界各地人们交流的绝佳场所。不幸的是，互联网也成为一个挑战主流语话的独立思考者经常发现自己受到攻击的空间。这些攻击可能非常个人化、具有强烈的针对性—— 因为互联网上经常会有很多关于我们的个人信息。

为了加强你对这些攻击的防御，从评估自己的数字阴影开始是个好主意。这些阴影—— 可以讲述一个关于我们的故事：我们是谁、我们生活和闲逛的地方、我们感兴趣的东西，以及朋友和同事都是谁。这可能会让我们面临几种威胁。特别是，你留下的公开可用数字足迹会导致你面临各种骚扰和操纵。

不过，你还可以使用许多策略和工具来塑造或控制自己的数字阴影，增加自己的隐私，并最终在线和离线时更加安全—— 并不会减少您的声音或在线活动。

这些例子包括通过有意识地从内容和元数据中剥离有价值的信息来控制自己被暴露的数据量；尝试自‘我毁灭“的艺术；并思考如何操弄和拆散自己的在线身份。

数字阴影都是什么？

数字阴影可以定义为数据说出的关于你的故事。这些数字阴影是由数万亿比特的数据创建的，当我们连接到互联网时，每天都会留下数字痕迹。你的数字阴影拥有自己的生命，受到他人的影响，并以不可预测的方式发生变化。这些痕迹是我们过去和现在活动的幽灵，它们以永久的和不断变化的形象融合在一起。

这些万亿比特的数据是如何创建的？我们用于浏览互联网、访问网站、连接到 Facebook 和 Twitter 等社交网络平台、发布博客帖子、接听电话、发送短信或电子邮件、使用聊天或在线购物的设备和软件，都创建了特定的位关于我们的数据。

这些数据可以包括我们的名字、位置、联系人、图片、消息、推文和点赞，还包括我们的计算机品牌、打电话时间和访问的网站的信息。这些数据痕迹可以由我们自己和其他人一起提供。

如何共享数据？在某些情况下，人们会积极分享数据—— 例如，当我们在 Facebook 上分享照片、在线预订机票或发帖子时。其他人也可以通过在图片中标记我们、在推文中提及我们、或仅仅通过与我们沟通来积极地分享关于我们的数据。

在其他情况下，我们每个人都在不知不觉中提供了大量的数据，而没有考虑是否“同意”。当你通过“cookies”和其他在后台活动的跟踪技术访问网站时，你的浏览习惯和IP地址是共享的。这些技术就嵌入在我们访问的网站中，并且从网站分析到广告，被收集的共享信息可用于广泛的目的。

手机应用程序也在你不知情或未经同意的情况下收集数据—— 例如，我们拍摄的照片通常会在其中嵌入位置数据。当从一种服务转移到另一种服务时，这些跟踪技术使 Web 服务能够识别和关注你。

什么是数据？数据可以分为三个部分：内容、元数据和噪音。

- 内容是我们的消息、博客、推文和电话的内容，包括照片和视频。元数据是关于数据的数据，是技术基础设施工作所需的信息。

- 元数据使我们的电子邮件能够交付，帮助在我们的计算机上查找文件并允许移动通信。元数据可以是我们的电子邮件地址，电话号码，位置，发送或存储消息的时间和日期。

- 噪声是由制造过程或基础设施的工作所产生的数据。例如，每台相机都有一张SD卡来记录和存储图片。每张SD卡都有独特的划痕，这些划痕是由生产SD卡的机器创建的。这些划痕会对眼睛看不到但可被计算机识别的数据进行微小的更改。

谁在收集我们的数据，为什么？

数据收集和数据分析已变得非常复杂。您遗漏的数据痕迹将由各方收集、分析和分类，以创建数字阴影或配置文件。每次收集新数据时，都可以识别并添加到您的个人资料中。这些配置文件不断扩展，为创建它们或有权访问它们的人提供了对您本人的真实洞察力。

公司、政府和个人为各种目的收集这些数据。它可以买卖；可以用来操纵和控制；或者可以用来制定骚扰策略。

数字阴影或配置文件可用于深入了解我们是谁、我们做什么、以及我们去过哪里。然后，可以使用这些数据来预测我们可能会做什么或将来可能会去哪里。例如，如果有人知道我们是x国家中关于性别问题的直言不讳的博主，他们就会知道我们可能会参加一个关于该国博客和女权主义的会议。配置文件还可以使潜在的骚扰者能够在不同平台上骚扰我们。

任何人都有可能访问你的数字阴影—— 包括通信服务提供商、执法机构和商业公司，以及运行自己的服务器的团体和个人。我们无法准确知道自己的数字阴影究竟发生了什么，而这本身就是一个问题。

但是，我们可以使用工具和策略来管理数字阴影、并限制其在剖析和监视方面的影响。后面就是用来讨论这一问题的。

探索你自己的数字阴影

正如之前提到的，任何人都可以访问你的数字阴影—— 包括通信服务提供商、执法机构和公司，以及运行自己的服务器的团体和个人。那么怎么办？建议从下面开始：

- 使用 Trace My Shadow 探索自己的个人数字阴影—https://myshadow.org/trace-my-shadow—这是由 Tactical Tech 推出的工具；

- 了解您是否可以更改手机中的访问权限设置。在 iPhone 上，可以在其隐私设置下更改每个应用的权限。

控制您共享的内容和元数据

好消息是我们可以部分控制我们提供的内容和元数据。

当在网络上发布内容之前，最好自问一下，你发布的内容是公开的还是个人的，以及谁可以访问它。即使这些信息与公共活动有关而不是与我们的个人生活有关，提到的名字或上传的图片也可能会让人联想到我们是谁、我们在做什么、在哪里做等等。希望定位你的人就可以使用它。

这并不意味着你应该保持沉默—— 只需采取一些基本措施，你可以通过提高攻击难度来减弱风险：

- 在必需分享有关自己生活的个人详细信息时，务必设置为仅仅所选的联系人可访问私人资料。在商业社交媒体上使用私人资

料时，应该了解该平台隐私政策的定期更改，这可能会影响我们的个人资料的“私密性”。

- 在网上和公共可访问的社交网络资料上撰写或发布有关公共活动的图像时，应该首先问自己，你传播的有关单个人、地点和其他细节的信息是否可用于识别和/或攻击某人。或者只在公共活动结束后才公布有关公共活动的信息。

- 可以使用名为 ObscuraCam 的工具匿名化图片中的面部，ObscuraCam 是 Android 设备的免费相机应用程序。

- 在向**Web**服务提供个人信息时，最好使用 HTTPS 以使通信通道安全。

- 使用强密码，并为您使用的每个 Web 服务使用不同的密码—— 如果您为多个服务使用相同的密码，并且有人拦截了其中一个服务的密码，就可以使用它来访问您的其他帐户。

- 注册 Microsoft Office，Libre Office，Adobe Acrobat 等设备或软件时，不要使用真实姓名有助于防止在使用此设备或软件时创建的元数据与您的身份连接。您也可以关闭手机或相机中的**GPS**追踪器。

- 某些文件类型包含的元数据多于其他文件类型，因此在线发布内容时，您可以将文件从包含大量元数据的文件格式（例如.doc和.jpeg）更改为不包含元数据的文件格式（例如.txt和.png），或者我们可以使用纯文本。

- 使用 Metanull for Windows 从图像文件中删除元数据。

- 编辑或删除 **PDF** 文件中的隐藏数据，Windows 或 MAC OS 用户可以使用 Adobe Acrobat XI Pro 等程序（可以使用试用版）。 GNU / Linux 用户可以使用 PDF MOD，这是一个免费的开源工具。但是，它不会删除创建或修改时间戳，也不会删除有关用于创建 PDF 的设备类型的信息。

- 有关从不同文件格式中删除元数据的更多信息，请参阅 [image]大清洗 - 扫荡危险区域：完美隐身 S04E07

- 您可以通过安装 Privacy Badger 或 Adblock Plus 等附加组件，以及监控自己的隐私设置、定期删除 **Cookie** 来阻止通过浏览器的跟踪和收集元数据。

- 使用 **Tor** 将隐藏特定的元数据，如我们的 IP 地址，从而增加在线匿名性。

社交领域

正如安全专家 Bruce Schneier 所解释的那样，“安全是一个链条，任何一个薄弱的环节都可以打破整个系统”。

我们每个人都属于多个社交领域—— 我们的工作或倡导网络，我们的家庭网络，朋友和团队。其中一些网络可能需要比其他网络更多的安全。

例如，我们可能倾向于为我们的工作或倡导活动提供更安全的沟通实践，但在社交网络上与朋友交互的安全性就会相对较低。这些领域相交可能会对我们的安全构成威胁。

如果你在所有领域中使用单一身份，则可以更轻松地收集到有关你的一切信息并识别出你的漏洞。

例如，如果你在社交网络中透露自己喜欢某种特定类型的游戏，并且使用了像 Emule 这样的 p2p 程序下载文件，那么想要调查你的工作或倡导活动的攻击者，就可能会通过欺骗你下载游戏而令你感染间谍软件。这是所有社交工程伎俩中最最简单的一种。也是为什么说很多失败都源于你说得太多了。

这个攻击者对你的倡导活动和政治立场很感兴趣，但他知道你在这部

分生活中增加了隐私和安全措施。同时攻击者也知道你对游戏的热爱（或任何一种偏好都一样）是数字弱点，因为这个网络没有加密。因此，攻击者就可以利用你生活中无法加密的这一部分来获得入侵其他加密部分的入口。

很简单，这就是因为你的工作—敏感部分 和 生活—不敏感部分，没能彻底分开的原因；也是为什么要一直强调分离你的社交领域，为不同领域选取完全不同的身份—— 彼此之间不要发生任何联系。这就是身份管理。

自我人肉

几乎所有人都知道人肉搜索是什么意思。Doxing（也称为“doxxing”或“D0xing”）描述了使用互联网上免费提供的来源追踪或收集有关某人的信息的方法。此方法的成功取决于攻击者识别有关其目标的有价值信息的能力，并将此信息用于他们自己的恶意目的。

Doxing 的前提是“你越了解你的目标，就越容易找到他或她的缺陷”。反过来看，对你来说就是：最了解的你的人是最危险的人。你应该努力让仅仅经过验证的极少部分亲密人了解你，并且你选择的对方必须是和你具有同样高层次的保护意识的个人。

就如 IYP 在社交工程演示中所强调的那样，骚扰者和潜行者会使用多种工具和技术来收集有关其目标的信息，但由于这些工具和技术大多是公开的且易于使用的，你也可以自己使用它们。 BACK https://web.archive.org/web/20200519011344/https://www.iyouport.org/%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86%EF%BC%9A%E5%86%B3%E8%83%9C%E7%9A%84%E6%A0%B9%E5%9F%BA%E2%80%8A-%E2%80%8A-%E6%8A%80%E6%9C%AF%E5%92%8C%E6%8A%80%E5%B7%A7%E4%BE%9D%E6%97%A7%E6%98%AF/

很有必要推荐这一工作，因为你很可能完全不知道自己在他人眼中是什么样，尤其是不知道自己在监视者和所有恶意行为者眼中是什么样。“自我人肉”工作就是让你看清自己的必要工作—— 它可以帮助

你就在线共享内容和方式做出明智的决定。

当然，这项工作也可用于识别他人，在你决定给予对方*完全信任*的权限之前，上述相同的工具可以帮助你判断是否值得给出这样的信任。

用于 doxing 的方法包括浏览档案、黄页、电话簿、和其他公开信息；查询 Google 或 DuckDuckGo 等常用搜索引擎；在特定服务中寻找一个人的个人资料；在公共论坛和邮件列表中搜索信息；或寻找目标已共享的图像（例如，可能还发布在另一个更个人的帐户中）；也可以简单地通过“whois搜索”查找网站所有者的公共信息。

您自己就可以使用这些相同的工具来探索其他人可以轻松找到的关于你的信息。

在开始探索这些 Web 服务并寻找你的数字自我之前，一个好主意是使用像 Torbrowser 这样的匿名工具。

我们将在本栏目的下一篇文章中介绍更多自我人肉工具和技巧。

[image]

删除你的过去，创建新身份

“一旦有什么东西在互联网上，它将保留在互联网上，因为互联网不会忘记”。这句话已家喻户晓。

你可能认为从社交网络和 Web 服务中删除某些敏感数据可能足以保护自己，但你不能轻易删除元数据。在我们的整个生活中—— 在我们所有的工作和个人领域—— 如果只使用一个身份—— 就已经创建了大量可用于描述或攻击我们的信息。

要避免这种情况的一个选择是：留下旧身份，并创建一个或多个新身

份—— 给每个社交域一个完全不同的身份角色。你也可能选择在其中某些领域使用自己的真实身份，在其他领域使用创建的新替代身份。

以下是当你开始做这件事时的基本注意事项：

- 当你开始创建新身份时，应该仔细选择每个身份的联系人，并避免与你用于不同活动的其他身份共享联系人。这样才能有效地创建单独的社交域，包括单独的帐户、邮件地址、浏览器配置文件、应用程序，甚至可能是设备。
- 重要的是：要确保你持有的各种身份不以任何方式相互关联、更不能与你的真实身份相关联。请记住，其中一些相关性可能很脆弱而你没有发现：例如，你是否使用真实的电话号码注册了一个新的假名 Gmail 帐户？这是在自己挖坑。
- 将你的每个额外身份视为潜在的一次性身份可能很有用，因为如果它们受到了损害，你就可以很容易地丢弃它们。
- 在适当的情况下，可以为新认识的熟人创建关于你的一次性身份—— 你可以使用介绍性配置文件在将其包含在更受信任的网络中之前，了解某人。

别急，后面还有更多具体介绍。

删除身份

如果你决定通过创建多个身份来区分自己的不同领域，那么你应该做出的第一个决定就是删除或保留你已经拥有的身份或特性。

要做到这一点，就必须从调查你的现有身份或特性的痕迹开始。也就是上面介绍的自我人肉。

以下是在你在删除的时候需要知道的：

- AccountKiller

https://www.accountkiller.com

提供了有关如何删除大多数热门网站上的帐户或公开个人资料的说明。

- JustDelete Me

http://justdelete.me

是一个直接链接目录，用于从Web服务中删除帐户。

映射你的社交域

为了区分你自己的不同社交域，就要首先将它们映射出来，并确定哪些可能使你最容易受到跨域攻击，这是很有帮助的。

你可以通过考虑自己不同的活动和网络来做到这一点，并反映每个活动和网络的敏感程度。这将使你能够更好地区分敏感域和非敏感域。

将一个人的数字生活划分为单独的普通社交域（或“机密安全”域）需要一些思考。

波兰计算机安全研究员 Joanna Rutkowska 就此进行了广泛的工作，是她开发的基于“隔离安全”概念（Qubes OS）的 Linux 发行版。

在此系统中，每个社交域都在一个单独的虚拟机中隔离。虽然 Rutkowska 的计划非常复杂并且专注于她的操作系统，但它可以为我

们提供有关如何开始考虑分离不同域的有趣见解。

Rutkowska 为自己确定的三个基本领域是："工作"，"个人"和"红色"（也就是不受信任的、不安全的区域）。

- 工作域包括她的工作电子邮件，在那里她保留她的工作 PGP 密钥，在那里她准备报告、幻灯片、论文等。她还有一个不太受信任的"work-pub"域，比如接受 LinkedIn 邀请或下载她的演示文稿的图片。为了增强这一点，她有一个"工作管理员"和一个"工作博客"域，以便进一步提高管理公司服务器的安全性并在她的博客上写作。

- 个人域包括所有与工作无关的内容—— 例如个人电子邮件和日历、假日照片、视频等。她为此增加了一个名为"非常个人化"的特殊区域，当她离家时，就用这个域与她的伴侣进行交流。这对夫妇使用加密邮件进行通信，为此目的，她有单独的PGP密钥。

- 红色域完全不受信任。这是她的一次性身份或简介所属的地方。Rutkowska 使用此域来执行不适合其他域的所有内容，并且不提供任何敏感信息。

- 除了这三个主要领域外，Rutkowska 还有其他几个独立的域。一个致力于购物，用于访问电子商务网站；定义此域的是访问她的信用卡号码和她的个人地址（用于运送）。然后是保险库域，她最终信任的地方，她生成并保留所有密码（使用 KeePassX）和主 GPG 密钥。最后，她拥有一个独立域为所有 Qubes development（"qubes-dev"）。

当然，你可能不必以如此复杂的方式分离自己的域，并且使用 Qubes Os 将它们分开只是一个解决方案—— 而且需要一个强大的机器来运行。

然而，**Rutkowska** 对域映射的思考方式完全可以成为分析我们自己的活动的启发性起点，并将我们的社交域分割开以增强安全性。

下图显示了不同域之间的数据流动：

[image]

你可以看到很多数据流都是从更受信任的域到不太受信任的域——例如，复制和粘贴在工作域中通过电子邮件收到的 URL ，以便可以在不受信任的红色中打开它，或者将通过电子邮件收到的发票从工作域发送到会计域。

但遗憾的是，还有一些数据流从不太受信任的域转移到更受信任的域。一个例子是复制和粘贴一个有趣的 URL，是刚刚在红色域中浏览时偶然发现的，你想与工作域中的同事或朋友分享，所以你需要将其复制并粘贴到工作（同事）或个人（朋友）域的电子邮件中。

现在，将数据从不太受信任的域复制到更受信任的域，是一个重大问题。虽然人们可以认为将 URL 粘贴到 Thunderbird 电子邮件编辑器是一个无害的操作，但它仍然是一个不受信任的输入；将更酷的图形文件从 Web 复制到工作域中的例子可能更可怕，只是为了在演示幻灯片中使用，通过恶意 JPEG 或其他图形格式发起的攻击，以及利用渲染代码中的漏洞已经存在有十多年了。

但是不幸的是，这个问题—— 如何处理从不太受信任的系统到更可信赖的系统的数据流—— 在实践中不容易解决。

不过，设计和构建供军方和政府使用的高安全性系统的一些人采取了一种相反的方式—— 他们说他们并不关心信任度较低的域向信任度较高的域的数据传输，只要他们能确保没有办法以相反的方向进行转移就行了。

因此，如果我们可以构建一个系统来保证更可靠的域永远不会将数据传输到不太受信任的域（即使这两个域都被泄露了！），那么他们很乐意允许单向“向上传输”。在实践中，这意味着我们需要消除两个合作域之间的所有隐蔽通道。合作这个词在这里是一个关键词，这使得整个想法根本不实用，恕我直言。

在该方案中确实需要消除合作域之间的隐蔽信道，因为假设来自较不可信域的数据传输确实可能危及更可信的域。

但至少，这不应该导致任何数据泄漏回原始域，不太受信任的域可能与之相联。这里的假设之一是这种系统的用户连接到多个孤立的网络。即使在那种情况下，消除域之间的所有隐蔽通道也是一个巨大的挑战，可能只有在我们准备好大大牺牲系统性能时才能完成。

可以肯定的是，不可能在不久的将来消除 Qubes 域之间的合作隐蔽通道。我只是不相信这种方法，也不喜欢这种方法无法保护更受信任的域的完整性—它只关注隔离方面。因此，攻击者可能无法将秘密泄露回较不受信任的域，但他或她可以在此更受信任的域中执行其他操作。如果我们不保持诚信，隔离有什么用呢？

这种传输的替代解决方案是拥有可以处理特定文件类型（如 JPEG）的可信“转换器”或“验证器”，并确保我们在目标域中获得非恶意文件。虽然这可能会让你想到旧的 A / V 技术，但它有所不同。

在这里，可信转换器可能是一些用安全语言编写的程序，运行在另一个受信任的域中，而不是一个丑陋的 A / V，其中包含一个巨大的数据库，包含可能出现在 JPEG 文件中的“坏”模式的签名。

这种方法的明显问题是有人必须编写这些转换器，并为我们希望允许转移到更可信域的所有文件类型编写。目前暂时忽略这个问题。或者说，根据使用者的个人风险评估（威胁模型）来决定该怎么做。

[image]

评估风险和潜力：如何选择适合我们目的的在线身份

“真实”还是虚拟身份？

一旦确定了不同的社交域以及与之相关的数字活动和联系人，你需要做的是决定是否要相应地区分自己的身份，或者是否愿意坚持自己的正式身份和真实面貌对他们每个人。

你可能希望将自己的工作与法律层面上的“真实”身份联系起来，或者认为行动主义应该是匿名的，这些是需要仔细考虑和衡量的决定。

例如，一名记者发现使用真实身份进行写作比较方便，那么就可能决定通过昵称与自己的个人域保持联系。另一方面，如果活动家一直在被政府追踪，决定使用化名进行在线活动，那么就应该考虑自己将在现实世界中所有相关活动中展示的身份，例如在会议上发言或参加示威游行。因此，她的在线笔名将与她的脸相关联；但她的脸也可能与她在社交网络上的真实姓名有关联，她的在线活动家身份也就被揭露了。

在评估在给定环境中使用哪种身份时，问自己以下这些问题会很有帮助：

- 如果我的真实身份在这种背景下被人知道，我的工作、生计或安全是否会受到威胁？
- 如果我被人知道参与了X活动，我的心理健康或稳定会受到影响吗？
- 如果我的真实身份在这种情况下被人知晓，我的家人或其他亲人是否会受到任何伤害？
- 我能够并且愿意安全地保持各领域不同的单独身份吗？

一旦我们评估了风险，就可以考虑在线分离自己的身份的不同策略。评估风险很简单，需要问自己：我要防御的人是谁？他们有什么技术能力？我最脆弱的地方在哪？我愿意为保护自己的资产和人身安全付出多少努力？

在线分离身份的策略

维护单独身份的策略范围可以从完全透明到完全匿名，不同等级。

作者 Kate Harding 谈到她决定以她的真实姓名开始写作，驳回了博主们通常会采取的建议，例如“以化名写作，如果你是一位女士，那就采用男性化或中性化”的博客……掩盖一个人的个人信息，谨慎地发布可识别性细节，不要写任何可能激怒疯子的东西“……

Harding 说，骚扰问题应该由包括男性在内的整个社会来处理，而不是让女性负责。这就好像部分中国的异议人士所说的：“政府不应该监视和骚扰我，而不是我应该为避免骚扰做什么”。这显然是不可能的。好在 Harding 也承认，实名的决定是非常危险的。

因此，我们有几种选择：可以尝试匿名在线参与，可以使用“持久假名”。或者只在有些时候使用真名，并在其他时间使用假名。以下将谈论每种方式的优缺点，以便您可以选择合适自己的方法。

匿名——

完全匿名既可以是孤立的，也可能是较难维护的，但是在我们不需要获得其他人更多的信任时、当我们可以信任的人很少甚至完全没有时，或者我们不希望自己暴露给其他人的情况下，它非常有用。

在某些特定情况下，匿名可能是一个不错的选择，例如研究或参与有关健康问题的留言板，或者在共享任何一种敏感信息时，尤其是政治。我们可能希望使用假名设置一次性帐户来评论博客或新闻网站，或者一次性电子邮件帐户或聊天会话以与他人讨论敏感信息。

不愿透露姓名的人权活动家写道：“我是一名普通的社交网络用户。我就一系列主题发表意见。我谈论的话题并不需要我暴露面孔和名字“。

匿名与“持久假名”并不同。当我们采用匿名作为策略时可能会使用假名，但这些假名不会在不同的网络或社交域中被使用，有些只能使用一次然后丢弃。

持久的假名——

持久性假名涉及在一段时间内持续使用假名。

牛津英语词典将化名定义为“虚构的名称，尤其是作者使用的名称”。在互联网时代，假名也可以被称为“昵称”或“称号”，尽管后者也可以与个人的合法身份产生关联。

Jillian C. York 在电子前沿基金会的博客文章中写道：“为什么个人可能希望使用他们出生时的名字以外的其他名字有很多原因。可能是担心对他们的生活或生计的威胁，或者可能冒着政治或经济报复的风险。可能希望防止歧视，或者可能会使用在特定文化中更容易发音或拼写的名称。“

假名可以是人名形式的（例如，“Jane Doe”）也可以不是。在撰写本文时，某些网站（包括 Facebook）要求用户使用其“真实身份”，这通常意味着使用您的法定名称或您熟悉的名称。该政策的推出令一些用户的账户被封锁。如果我们选择在社交网络上使用假名，重要的是要了解这样做的风险：避免这种情况的策略是使用看起来像真人名字的假名。

不必担心，持久性假名也可以提供可见性。可见性使我们能够与他人建立联系，通过将我们的声音固定到特定名称上，同样可以建立在线声誉。在线声誉允许其他人决定我们是否值得信任，因此是基于信任的在线社区的关键方面。

当然你也可以通过始终使用与自己的合法身份相关联的昵称或假名来开发声誉。但要知道，将在线声誉与“真实”名称联系起来的选择应根据需要和具体背景酌情而定。

为了不同的目的，也可以保留多个假名、和多个领域的声誉。

集体身份——

另一种匿名方式是通过集体参与。这可能意味着许多事，从发布集体声明的私人团体或邮件列表、到共享的 Twitter 帐户。就如 IYP，我们并不是一个人，但我们所有人都称为 IYP。

虽然同样的安全问题在这里也适用，但在集体身份背后工作意味着你拥有人群的力量，如果您不想透露自己的身份，这可能是一个不错的选择。

比较策略——

无论我们做出什么样的选择，重要的是我们保持自己的不同空间域有效分离。

无论你在数字生活中存在多少不同的领域、以及创造了多少相应的身份，在互联网上，每个身份—— 即使是带有真实姓名的身份—— 都会变成“虚拟”角色，应该谨慎管理它们每一个。

各种身份选择的利弊：

[image]

创建新的在线身份

1、起个名字

起名因文化而异。虽然名称以某种形式可以存在于不同的文化之间，但是“法定名称”的概念是一个相当新的概念。

不同的国家以不同的方式规范命名的做法。例如，在摩洛哥，名字必须从政府批准的名单中选择，而在德国，名字必须明确反映婴儿的性别。

在互联网上，具有“实名”政策的平台倾向于据此判断基于个人的法定名称，而不是允许他们根据自己的选择进行识别。这可能是有问题的，不仅对于试图保持匿名的个人来说，而且对于变性个人、具有别名的个人和其他人来说都很麻烦。

由于这些限制，在选择假名时选择那些看起来像真人的名字可能是有益的。尤其是使用商业社交网络时，最好使用可靠的名和姓，而不是更富有想象力的名和姓。

一旦决定了虚拟角色的名字、姓氏和用户名，就应该进行彻底的研究—— 也许还要使用自我 doxing 的工具和技术（参见前面）—找出其他人是否已经在使用该名称。毕竟，如果我们希望发展自己的声誉，不希望与别人混淆，特别是如果他们不同意我们对世界的看法的话。

2、写自己的故事

“故事讲述”（以及为此创建社交面具）的做法是很有传统的，并且创建一个带有故事的新角色使得维护角色变得容易得多。

重点是，当我们创造一个身份时，应该设想一个完整的虚拟角色，一个需要培养和发展的化身，才能变得可信。

3、创建在线资料

一旦创建了几个角色，重要的是让它们将你的现实生活和数字生活中分开。虽然记录身份可能有助于确保你记住自己的故事，但也可以采取技术措施来确保我们的个人资料保持独立。

一个好的开始是为自己的每个身份创建不同的浏览器配置文件、邮箱和社交网络帐户。一个好的经验法则是始终为每个帐户/身份使用不同的应用程序，如果可能的话，为每个身份分配不同的设备或操作系统。

4、创建单独的浏览器配置文件和邮箱

浏览器配置文件：使用 Firefox 创建多个配置文件。

邮箱：创建新邮箱时，最好使用 Torbrowser 连接到服务器的网站，如果需要联系电子邮件地址，请考虑使用一次性电子邮件地址。

5、在社交网络上管理身份

建议始终使用安全的 HTTPS 连接。

– 在社交网络平台上为新角色创建帐户时，请使用您为该角色创建的浏览器配置文件。

务必检查隐私设置，以便了解您公开了什么、谁可以查看您发布的内容、谁可以与您联系、谁可以查找您、以及您的联系人可以做什么（他们可以在图片中标记您吗？等等）

– 同时要非常小心您提供的个人资料信息，以及您使用的个人资料照片和封面照片。

因为无论隐私设置如何，这些信息通常都会公开给在该社交网络中查找你的任何人。IYP 的社交工程演示中曾多次使用过头像和封面照片作为线索。

– 确保您的虚假身份联系人不与其他身份重叠，并确保您的不同身份间不会彼此关注。

切勿使用您的真实身份账户关注您的假名账户。如果有人想要揭开这些人物角色中的一个角色的真实身份，他们首先要寻找的就是该帐户所关注的人以及谁关注该帐户。出于同样的原因，我们应该避免将一个帐户发布的帖子或其他内容在另一个帐户重新发布，更不要互相转发。

– 大多数社交网络平台都会尽可能地显示您的位置。

当你使用支持GPS的手机与平台进行交互时，通常会提供此功能，但如果你从其他设备连接也会发生这种情况—— 例如，计算机所连接的网络也可能提供位置数据。请仔细检查您的设置—— 特别是在照片和视频共享网站上。

– 照片和视频也可以在您没有意识到的情况下显示大量信息。

许多相机会将元数据嵌入到您的照片中，其中可能包括照片的日期、时间和位置、相机类型等。当我们将内容上传到他们的网站时，这些信息就会被暴露。

– 如果通过移动应用程序访问社交网络平台，最好为每个单独的帐户使用不同的应用程序，以免错误地将内容发布到错误的帐户。

有几个应用程序可用于管理您的社交网络平台—但是，为每个身份使用不同的应用程序始终是一个好主意，以降低泄露您的真实身份的风险。

– 在一天中的不同时间使用您的不同身份发布。

一些社交网络平台，如 Facebook，允许用户安排帖子的发布时间。Postcron（https://postcron.com ）也可以帮助您在 Twitter 和其他平台上安排定时发布帖子。

– 为了进一步将你的真实身份与你的假名身份保持距离，你还可以在假名配置文件中写下（并在 Twitter 上发布相关主题标签）关于你从

来没有参加过的事，特别是如果这些事发生在远离你所在地的地方。发布它们然后删除那些看似已经暴露了“真实身份”的帖子，也会很有趣，这样可能会让任何试图揭露你真身的人感到困惑。

– 无论决定使用哪种社交网络平台，您都应该仔细阅读其服务条款，以检查它们是否适合您的目的。

6、另类社交网络

如果你的目标是尽可能广泛地宣传自己正在组织的活动或正在推出的项目，那么主流商业社交网络平台（如 Facebook 或 Twitter）有可能比较有用。

但是，如果您正在使用其中一个主流平台，请务必注意：

- 这些平台有非常严格的审查条款，如果他们发现你的内容“违反”了他们的规则，他们可以随意封锁你的帐户；
- 它们会对用户进行概要分析，并将信息出售给广告商。这使得很难清楚地了解你的数据实际发生了什么，最好的解决方案是将商业社交网络平台的使用限制为特定的、仅希望向广大受众宣传的内容。也就是，此外别的话不要说。

当然，你还有其他可用的选择—— 为用户提供更多自由的平台。

- Ello 在其宣言中明确指出“你不是产品”。它也不需要你的“真实姓名”—— 在商业社交网络中很少见。然而，重要的是要注意 Ello 仍然是一个商业项目。
- 基于免费开源软件以及对隐私友好的分布式而非集中式的替代方案，是更重要的。其中，Diaspora（https://joindiaspora.com），Friendica（https://friendi.ca）和 Crabgrass（https://we.riseup.net）更值得一提。

- 还有其他类似的网站可能在不同的地区很受欢迎，所以希望您探索其他选择。

在选择使用社交网络平台之前，你应该问以下问题：

- 它是否为网站的所有用途提供了基于 SSL（如 HTTPS）的连接，而不仅仅是在登录期间？是否存在与加密相关的问题（例如与加密证书相关）？

- 根据平台的最终用户许可协议、隐私政策和/或数据使用政策，您的内容和个人数据将被如何处理？与谁分享？

- 为用户提供了哪些隐私选项？例如，我们可以选择仅与少数人安全地分享视频吗，还是默认情况下都是公开的？

- 服务器的地理位置是否已知？属于哪个属地管辖权？公司在哪里注册？这些信息如何与我们的活动和信息的隐私和安全相关？

7、创建博客或网站

你可能需要一个更独立的平台来传播想法、计划或创作。为此，可以创建一个网站或博客。

- 创建博客就像注册博客平台并选择名称和“主题”或可视化模板一样简单。有几个博客平台既方便用户又免费，包括开源 WordPress（WordPress.com）。

- 另外面向安全的平台还有：**Noblogs** (http://noblogs.org/) 和 Nadir’s **BlackBlogs**—(http://blackblogs.org/). 要在这些平台中的任何一个上创建博客，只需在服务器上托管电子邮件帐户即可。

- 如果想要复杂的图形布局、或需要安装 WordPress 及其插件不提供的特定工具，可以创建自己的网站。A / I 是个选择，默认情况下不会将其服务的用户与真实身份相关联。

- 如果想使用自己的域名，除非使用比特币或其他匿名支付系统，否则绕过支付的身份识别可能会很困难。我们将提供的个人数据不仅存储在注册商的内部档案中，而且默认情况下任何人都可以通过搜索引擎（whois）或 Gandi. net 中的简单命令轻松查询这些数据。这时候也许你需要挂名一个组织并使用他们的信息，或者可以使用像 Gandi.net这样的注册商，它可以尽可能为个人提供私人域名注册。

[image]

管理集体在线身份

1、集体虚拟角色

General Ludd, Captain Swing, the Guerrilla Girls, Luther Blissett, Anonymous—— 几个世纪以来有很多志趣相投的人们组建团体匿名参加了历史性的抗议活动，或者以集体笔名创造了突破性和挑衅性的艺术品或恶作剧。除了隐藏所涉及的个人的身份之外，这些集体角色已经在近乎神奇的光环中笼罩了他们所有的壮举。

如果我们想采用集体身份，可以采用已存在的身份，如 Anonymous / Anonymiss，也可以创建一个我们可以共享的新身份。

- 关于集体认同的一项非常有趣的研究是人类学家 Gabriella Coleman 的书《Hacker，Hoaxer，Whistleblower，Spy. The Many Faces of Anonymous》IYP 介绍给这本书，基于对匿名者如何成为具有多种面孔和态度的众所周知且强大的集体认同的人类学研究。

- 在 《Networked Disruption. Rethinking Oppositions in Art,

Hacktivism and the Business of Social Networking (2011)》中，Tatiana Bazzichelli 描述了多重身份是如何被用来破坏权力和霸权的基本概念，以及它如何在今天的网络中发挥重要作用。

2、管理集体身份……或简单的集体账户

虽然许多人的合作可以帮助创建一个丰富的集体身份，但管理一个集体项目可能会有一些你应该记住的安全和技术挑战。

由于安全链中的单个弱连接都可能会破坏整个系统，因此我们的安全性和匿名性取决于我们小组的每个成员所采取的预防措施。安全是一种集体思维。我们的团队能获得的安全程度取决于我们可能面临的威胁、以及我们对手的力量和技能。

尽管如此，你肯定不希望丢失一些重要的东西，例如你的集体邮箱或集体使用的社交网络帐户的密码。如果你决定与整个团体共享这些密码，则需要对每个成员进行如何安全存储密码的培训。

为了最大限度地降低此类风险，应尽量使用提供不同帐户和密码的服务。例如，可以创建一个所有成员都订阅的邮件列表，而不是使用单个邮箱。如果允许未订阅的人员写入，则每个组成员都能够在他们自己的邮箱中读取该电子邮件，而不是在具有危险共享密码的集体邮箱中。

同样，如果真的需要通过 Facebook 进行协调，那么在专门的小组中共享信息要好得多，而不是在集体账户中做所有的事。

每个身份的不同设备——

如果你对自己的几个身份使用相同的操作系统，无论如何谨慎地分离配置文件，仍然会犯下人为性的错误，例如，连错了账户，或者被恶意软件感染，允许攻击者使用我们的所有身份监控我们在线做的所有

事。

通过为每个域使用不同的虚拟机，以及通过保留另一个虚拟机来打开不受信任的附件以避免恶意软件感染，可以限制这两种风险。

出于匿名化的目的，最好的选择是安装 Virtualbox，一个开源的跨平台虚拟机监视器（https://www.virtualbox.org）。使用 Virtualbox，您可以创建一个虚拟机，然后在其上运行一个名为 Whonix 的操作系统。

Tails——

如果拥有自己的计算机，可以自由安装任何我们想要的东西，特别是如果它是一台功能强大的机器，那么使用虚拟机，特别是 Whonix 是一个好主意。但是，如果我们使用较旧的机器或只是从网吧连接到互联网，安装虚拟机就不行了。在这种情况下可能会转向一个安装了 Linux 操作系统的 USB 记忆棒，只要打开它就会在正在使用的计算机上运行。

这种情况下推荐 Tails，或 Amnesic Incognito Live System，这是一个基于 Debian 的免费开源 Linux 发行版，几乎可以在任何计算机上通过 DVD，USB记忆棒或SD卡启动。强制所有传出连接通过**Tor**，阻止直接的非匿名连接。

这是一个完整的操作系统，就像 Whonix 一样，配备了几个内置应用程序：Web浏览器，即时消息客户端，电子邮件客户端，办公套件，图像和声音编辑器，等等。使用 Tails，可以访问互联网，进行通信，并完成所有我们需要的匿名和安全操作，并且在计算机关闭后，系统将不会在机器上留下任何痕迹，除非我们要求它这样做。

使用不同的身份时，不建议使用相同的 Tails 会话执行两个任务或认可两个身份。第一个原因是Tor倾向于重复使用相同的线路，例如在相同的浏览会话中，使得强大的对手更容易将多个浏览请求关联为同一线路的一部分并且可能来自同一用户。其次，如果在使用 Tails 或其中一个应用程序时出现安全漏洞或误用，可能会泄露有关我们会话

的信息。

这两种威胁的解决方案很简单，就是每次使用新身份时关闭并重新启动 **Tails**。

隔离安全性：**Qubes OS——**

数字安全有三种方法：第一种是模糊的安全性，它基于加密、强密码和类似的措施，并作为第一道防线；然后是正确的安全性，软件开发人员试图摆脱使他们的代码易受攻击的 bug。但现代软件非常复杂，几乎不可能完美地完成这项工作。因此，最现实的方法是隔离安全，理所当然地认为安全措施可能是脆弱的，并通过阻止可能的攻击者访问我们想要保护的整个系统来减少伤害。

例如，为了通过隔离实现安全性，Whonix 分为两部分：Whonix-Workstation，以及 Whonix-Gateway，它通过 Tor 路由所有互联网流量，并通过与前者分开，避免恶意软件、行为不当的应用程序和用户错误带来的许多威胁。

如果你不想要 Whonix 呢？有一个操作系统通过以隔离作为其主要目的而具有安全性，并且可以使管理多个社交域和/或身份的人的生活变得更加容易。

它被称为 Qubes OS—

https://www.qubes-os.org

由计算机安全研究员 Joanna Rutkowska 开发， Qubes（https://www.qubes-os.org）是一个免费的开源安全导向操作系统，基于 Fedora，Linux 发行版和 Xen，它允许我们将数字生活的各个部分分离为安全隔离的虚拟机。

Qubes 将我们在计算机上执行的操作安全地隔离在这些不同的VM 中，这样，如果一台虚拟机受到攻击，另一台虚拟机也不会受到影

响。

通过这种方式，我们可以在一台物理计算机上完成所有工作，而不必担心一次成功的网络攻击会损害我们整个系统，也不会有人能够揭示我们几个身份之间的所有联系。

用于多个身份管理的 Qubes OS 的优势在于其用户友好的窗口管理器，它为每个域分配不同的颜色。因此，框架的颜色使得每个窗口清晰可识别为属于对应于该颜色的域，并防止你在身份管理中潜在的人为错误。

那么 Tails，Whonix，Qubes OS：应该如何选择

Wonix，Tails 和 Qubes OS—都允许我们使用完全独立的操作系统来管理我们的替代身份，并且可以非常有用。当然，选择取决于您可以用来保护数字生活资源和切实的威胁模型，尤其是您期望面对的对手：如果你面对的是国家政权，那么绝对要肯定自己的数据都没有泄露。所以请先评估自己的资源和需求，以便确定最佳解决方案。

Tails，Whonix 和 Qubes Os 之间的比较如下：

[image]

好了，现在您知道哪一个最适合自己了。

最重要的是，不应将它们看作是一种万能神药，最重要的依旧是人—— 操作安全重于一切，而不是软件安全。但可以肯定的是，根据您的需求和资源，通过使用它们中的任何一个，都可以减少被攻击的可能性。

安全应该进入习惯，就像您使用右手签名还是左手那样自如。祝好运。

[image]
[image]

自我人肉

[image] 关键词	个人 反侦察 反追踪 对抗性思考方式 数字足迹 清理 自检 防御
[image] 关联	[image]大清洗 - 扫荡危险区域：完美隐身 S04E07
[image] 创建时间	2019年8月21日
[image] Description	操作安全性

你对目标的了解越多，找到他或她的弱点就越容易，然后就可以利用这些弱点以发起最有效的攻击。

- Table of Contents

  基本步骤是这样的：
  挖真实姓名
  政府资源
  谷歌 **Dorks**
  搜人
  搜用户名
  Google Dorks
  用户名搜索
  电子邮件地址
  Google Dorks
  电邮工具
  被攻破的数据库
  电话号码
  PhoneInfoga ——
  Android 模拟器 ——
  域名
  Google Dorks
  Whois
  反向 Whois

相同的IP
被动 DNS
Internet 档案和缓存
‘可靠吗’分析
物联网搜索引擎
位置搜索
地理定位工具
基于**IP**的地理定位
图
SOCMINT
自动化开源情报
SpiderFoot ——
theHarvester ——
Recon-ng ——
Maltego ——
FOCA ——
Metagoofil ——
总结

[image]

您对自己的弱点很可能不那么了解，而敌人却很了解。如果你想要防御敌人，那么就最好能首先”变成”自己的敌人 —— 通过他们的眼睛来看自己。

请注意，任何人都可能成为你的敌人 —— 而不仅仅是政府，还包括收钱“办事”的家伙。

最近我们惊讶的得知，早年只在欧美国家流行的私人侦探业务，目前也在中国出现 ；如下图，这是一家做相关业务的团队发布的简易版广告：

[image]

你往往不会知道自己在什么时候会得罪什么人。唯一的方法是：提前预防。

这就是“自我人肉” 系列的目的 —— 帮助您在被对手找到之前，尽可能砍断一切追踪线索。

正因为当下数字时代，人们在互联网上暴露了自己太多私密隐情，于是，社交媒体和互联网是追踪者首先会深入探索的。

这是一场竞技。你和你的对手谁先入手，谁就能取得胜利。

“自我人肉”系列将提供绝大多数追踪者都会使用的技术和工具，是的他们整天都在研究这些东西。现在，我们必须让大众了解这些东西，以便采取针对性的防御。

[image]

返回：[image]了解追踪者的手段和你的弱点：完美隐身 S04E02

返回：[image]大清洗 - 扫荡危险区域：完美隐身 S04E07

随着社交媒体的使用量几乎接近饱和，当权者对社交媒体情报的热衷一直在迅速膨胀；加之全网挖掘技术 如🔍开源情报 的兴起，并且工具越来越好用和自动化，几乎任何人都可以扒光你。

[image]

于是想要保护自己的人最有必要做的就是在被别人扒光之前，先自行找到针对自己来说最致命的东西，然后尽可能隐藏它们。

🔍开源情报 就是这样一种东西，它不仅能进攻而且也能防卫，如果你能在你的对手使用这些技术瞄准你之前，使用同样的技术对自己进行全面审视，就能发现对手最可能从哪里下手，便能做到有针对性的防御。

试试看，也许您能发现互联网有多可怕。也能知道自己或朋友是如何被警方抓到的。

有很多🔍开源情报 工具可供使用，本文不打算全部介绍它们，只讨论最常用的工具、以及在所描述的用例中比较有用的工具。

本指南会展示一种通用方法，您当然可以使用不同的工具和方法，具体取决于您的需求和初始状态。

基本步骤是这样的：

- 从您所知道的开始（电子邮件、用户名等等）
- 定义需求（你想得到什么）
- 收集数据
- 分析收集到的数据
- 根据需要使用新收集到的数据进行分析
- 验证你的假设
- 生成报告

下面分头介绍不同部分的挖掘。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

挖真实姓名

[image] IntelTechniques.com OSINT工作流程图：真实姓名

政府资源

有许多网站，您可以在其中找到有关人员或组织的信息，根据国家/地区的不同，信息开放性可能会有所不同。

本文不会列举所有国家的政府资源，因为作为不同国家的居民它们可能与你不相关。

但请记住，这些资源均在线，并且 Google 就能挖出来，它们并不难找，特别是使用运算符搜索的情况下。 BACK https://iyouport.substack.com/p/d91?utm_source=publication-search

谷歌 Dorks

2002年，Johnny Long 开始研究谷歌搜索查询，揭露易受攻击的系统或易于披露的敏感信息。他把这些方法标记为 Google Dorks。

现在，您可以通过数千种不同的查询来探索 Google Hacking Database。下面的查询可以通过简单的搜索返回给您原本难以找到的信息。

- *"john doe" site:instagram.com*—引号强制 Google 在 Instagram 上进行搜索时完全匹配。
- *"john doe" -"site:instagram.com/johndoe" site:instagram.com*—隐藏目标自己帐户中的帖子，但在其他人的 Instagram 帖子上显示发布的评论。
- *"john" "doe" -site:instagram.com*—显示与给定姓名和姓氏完全匹配但组合不同的结果，并从结果中排除 Instagram。
- "*CV" OR "Curriculum Vitae" filetype:PDF "john" "doe"*—在名称中搜索包含"CV"或"Curriculum Vitae"的目标简历，并具有PDF扩展名。

如果您对拼写有100%的肯定，请将单个单词用引号括起来。默认情况下， Google 会尝试将您的关键字塑造成大众想要的内容。

顺便说，Instagram 的有趣之处在于如果你使用正确的 Google Dork，甚至可以看到私人帐户的评论和点赞。

[image]

必须推荐同时使用 Bing、Yandex 和 DuckDuckGo 上的高级搜索查询执行搜索，因为其他搜索引擎可能会为您提供 Google 无法获得的结果。

搜人

有专门从事人物搜索的网站可以提供真实姓名，用户名，电子邮件或电话号码。

- https://pipl.com
- https://www.spokeo.com
- https://thatsthem.com
- https://www.beenverified.com
- https://www.fastpeoplesearch.com
- https://www.truepeoplesearch.com
- https://www.familytreenow.com
- https://people.yandex.ru

中国有一个“找人网 zhaoren.net”，也是足够可怕的；还有手机号、身份证号、IP地址等查询功能的“ip138.com”。

即便你移除了自己，新的搜索依旧会把你的资料包含在列表中。原因是不同的服务购买和使用了相同的数据集。于是您只需要等待一个更新的数据集出现。

相对的，您的侦查对象在站点A上删除的数据可能会在站点B上被找到。

搜用户名

首先，必须找到一个用户名。通常是名称加姓氏的组合、或源自该人使用或拥有的网站的域名。

从您拥有的数据开始，然后针对您的需求进行反向查找。

显然，最简单的方法是谷歌目前已知的任何相关数据，并尝试使用用户名查找任何页面。

此外，您可以使用反向用户名搜索的特殊网站，例如 socialcatfish.com，usersearch.org 或 peekyou.com。

Google Dorks

在搜索用户名时 Google Dorks 非常有用。此外，URL 搜索可能会给您带来良好的结果，因为通常URL包含用户名。

- *inurl:johndoe site:instagram.com*—在 Instagram 上搜索包含“johndoe”的网址。

- *allinurl:john doe ny site:instagram.com*—在 Instagram URL 中找到带有“john”、“doe”和“ny”字样的页面。与 inurl 类似，但支持多个单词。

根据搜索的复杂程度以及使用以前方法的成功程度，您可能希望生成一个单词列表。

当需要尝试很多选项时，列表会很有用，因为你没有清楚地了解用户名应该是什么，但是有很多猜测。

```
MacBook:usernames$ python usernames.py Names.txt
johndoe
doejohn
john.doe
doe.john
doej
jdoe
djohn
j.doe
d.john
john
doe
MacBook:usernames$
```

用户名搜索

很多网站都有用户名搜索，其中最好的网站之二是：instantusername.com 和 namechk.com。

通常，一个服务可以找到其他服务没有找到的东西，因此最好同时使用这两个。

除了在线服务外，您还可以使用 WhatsMyName—一个 Github 项目，包含更高级的工具：Spiderfoot 和 Recon-ng。但是，您可以将其用作运行 Python 脚本的独立检查程序。

您可能会得到误报，因为其他人可以使用相同的用户名，要为此做好准备。

[image]

请注意：高度建议全程使用匿名方法隐藏您的操作者身份。

电子邮件地址

[image]

Google Dorks

- *“@example.com” site:example.com*—搜索给定域名上的所有电子邮件；

- *HR “email” site:example.com filetype:csv | filetype:xls | filetype:xlsx*—在给定域上查找HR联系人列表；

- *site:example.com intext:@gmail.com filetype:xls*—提取电子邮件ID。

电邮工具

- Hunter—对电子邮件地址执行域名快速扫描并显示其常见模式。

- Email permutator—支持多个变量输入以生成自定义结果。

- Proofy—允许批量电子邮件验证，这在您使用排列工具生成电子邮件列表并希望一次性检查所有电子邮件时非常有用。

- Verifalia—无需注册即可免费验证单个电子邮件地址。要使用批量验证，您必须注册。

被攻破的数据库

数据泄露已成为一个大问题，最近我们看到越来越多的数据转储。

安全研究员 Troy Hunt 收集了被泄露的数据，剥离了密码，并将其上传到了 haveibeenpwned.com。

虽然违规事实本身可能不那么重要，但重要的是，知道您正在研究的人的电子邮件就可能获得该人使用的或至少曾经用过的服务列表。

另一种选择是使用 dehashed.com 。使用免费帐户时它的工作方式与 Troy Hunt 类似，但订阅版可以以明文或哈希形式显示密码。

从🔍开源情报 的角度来看，我们需要搜索它是否在其他一些网站上使用，另一种方法是找出该人使用或至少使用过哪些服务。

通过密码或其哈希进行搜索不仅可以显示使用过的网站，还可以显示与之关联的电子邮件地址。

因此可以获得使用其他方法无法获得的目标电子邮件。重要的是要注意，如果密码不是唯一的，可能会得到误报，因为其他人也可能会使用它。

电话号码

[image]

有时人们会将电话号码和电子邮件放入 Facebook 个人资料里，因此在 Facebook 搜索中键入这些东西就会显示个人资料。

另一个选择是查找用户提供的电话号码数据库，如 whocalledme.com 。

数据库不仅限于美国，也可以检查来自欧洲的数据。

此外，在移动设备上也有几个应用程序：privacystar.com，

getcontact.com 和 everycaller.com。

有许多反向电话查询服务，它们通常是针对特定国家/地区的，因此找到适合您需求的服务很重要。

PhoneInfoga ——

PhoneInfoga 是扫描电话号码的免费类最先进工具之一。

目的是首先在任何国际电话号码上收集基本信息，如国家、地区、运营商和线路类型，并且准确性非常高。然后尝试确定 VoIP 提供商或在搜索引擎上搜索足迹以尝试识别号码所有者。

- 检查电话号码是否存在且是否可行；
- 收集国家、线路类型和运营商等标准信息；
- 一次可检查多个号码；
- 使用外部 API，Google Hacking，电话簿和搜索引擎进行 OSINT 侦察；
- 使用自定义格式进行更有效的开源情报侦察。

Android 模拟器 ——

许多 Android 应用程序可以在模拟器上运行而不会出现问题，但有些可能无法按预期运行。例如，测试时，Viber 在激活 VoIP 电话号码方面存在问题。

但是，在模拟器上运行应用程序有很多优点：您的真实帐户或电话号

码将是安全的，因为您不必在手机上安装有问题的应用程序，并且您可以轻松欺骗GPS坐标。

将号码保存在手机中，然后查看 Viber 或 WhatsApp 联系人列表。这些服务允许添加照片、简介、所有者的姓名、并且只需知道电话号码即可提取此信息。

- Bluestacks—主要面向游戏玩家，但也运行其他应用程序。适用于 Windows，Mac 和 Linux，不需要虚拟机，因此安装比 Genymotion 更容易。

- Genymotion—被开发人员广泛使用，但也有免费版供个人使用。适用于 Windows、Mac 和 Linux，并有一系列虚拟设备可供选择。

- AMIDuOS—仅适用于 Windows，并利用系统中的设备驱动程序在 Android 中启用近乎原生的性能。它速度快，安装简单。然而要花钱，AMIDuOS 的售价为10美元。

域名

[image]

如果你想要的个人或组织拥有一个网站，你必须知道如何获取有关它的信息。

这一调查可能会揭示正在使用的操作系统、软件版本、个人联系信息等。

建议在没有“触及”目标环境的情况下进行调查，这种技术被称为被动侦察 —— 可以帮助获得有关目标的更多信息，而无需直接与其进行交互。

下面描述一些在保持隐身的同时获取信息的方法。

Google Dorks

以下是一些可用的查询：

- *site:example.com*—将搜索限制为特定网站或域。
- *filetype:DOC*—返回DOC文件或其他指定类型，例如 PDF，XLS 和 INI。通过用“|”分隔扩展名，可以同时搜索多种文件类型。
- *intext:word1*—找到包含您要搜索的特定单词的网页和网站。
- *allintext: word1 word2 word3*—搜索页面或网站中的所有给定单词。
- *related:example.com*—将列出与指定网页“相似”的网页。
- *site:*.example.com*—显示所有子域。 Asterisk 可以替代搜索查询中的单个或多个单词。

Whois

Whois 提供有关 Internet 资源的注册用户或受理人的信息，例如域名、IP地址或自治系统。

有许多 Whois 资源，这些资源都很好：whois.icann.org 和 whois.com。

反向 Whois

Reverse Whois 为您提供 Whois 记录中具有相同组织名称或电子邮件地址的域列表。

例如，如果您正在调查名为“John Doe Inc”的公司，您可以看到在“John Doe Inc”下注册的所有其他域名。

viewdns.info 很棒，因为它有一个广泛的工具包，包括反向 whois 查找。

相同的**IP**

在与目标网站同一台服务器上运行的网站中会发现有价值的信息。例如，您可能会找到子域或开发站点。

托管此站点的服务提供商通常也托管其他服务，请使用类似 AtSameIP 等工具进行检查。

被动 **DNS**

仅使用 DNS 记录有时还不够，这就是被动 DNS 派上用场的地方。

RiskIQ Community Edition 是值得推荐的，因为它提供的信息不仅仅是被动DNS。VirusTotal 或 SecurityTrails 也可用于此目的。

Internet 档案和缓存

The WaybackMachine 可用于查找以前版本的网页，使人们可以查看网站之前的状态或恢复已删除的网页。

Archive.today 是另一个网页时间包，可以手动将实时网址快照添加到存档。

有些情况下，已删除的页面未被归档但仍由搜索引擎缓存。可以在 cachedview.com 上找到它们，也可以使用以下 Google 查询请求缓存版本：cache:website.com.

在 Google 上没有找到任何内容吗？那就检查其他搜索引擎的缓存，但请记住缓存显示上次索引页面的时间。因此，您可能会获得包含缺失图像和过时信息的页面。

您可能还喜欢 visualping.io —一种监控服务，它在选定的时间截取网页的屏幕截图，并在发生变化时向您发送电子邮件警报。

‘可靠吗’分析

知道自己正在与谁打交道、以及网站是否可以信任，非常重要。

如果有任何疑问，请使用免费在线工具进行恶意活动检查，就可以会省去在VM中打开网站或执行其他预防措施的麻烦。

尽管单独进行测试并不能获得完全精确的结果，但它仍然是主要方法之一：

- www.siteworthtraffic.com —分析网站流量（用户，网页浏览量）并估算通过广告可以产生多少收入。
- www.alexa.com —分析网站流量和竞争对手，并提供有关SEO改进的建议。
- www.similarweb.com —分析工具，提供有关网站或移动排名、性能、流量来源等深层信息。最重要的是，它进行了referral analysis。
- https://sitecheck.sucuri.net —扫描网站上的已知恶意软件、

黑名单状态、网站错误和过时的软件。

- www.quttera.com —提供免费的恶意软件扫描，并提供包含恶意文件、可疑文件、黑名单状态等的综合报告。

- www.urlvoid.com—帮助您检测潜在的恶意网站。此外，它还提供了有关 IP地址、DNS记录等更多信息，并将其与已知黑名单进行交叉引用。

物联网搜索引擎

IoT（物联网）搜索引擎向您显示连接到网络空间的设备，就像谷歌搜索一样。为什么有用？

例如，您可以请求已有的有关开放端口、应用程序和协议的可用信息，而不是使用 Nmap 主动扫描端口和服务。

Shodan.io 是最受欢迎的扫描仪，具有公共API并与许多安全工具集成。对于营销人员来时，它提供有关产品用户及其所在位置的数据。

安全研究人员使用它来发现易受攻击的系统并访问各种物联网设备。还有其他替代品，如 Censys，或者它的中国复制版—Fofa 和 ZoomEye。

位置搜索

[image]

地理定位工具

Creepy 是一个免费工具，允许从社交网络和图像托管服务收集数据进行位置研究。

商业选择是 Echosec，每月花费近500美元，但如果您是非营利组织或自由撰稿人，您可以申请免费访问 Echosec Pro。

基于IP的地理定位

基于IP的地理定位是IP地址或MAC地址到真实世界地理位置的映射。

有许多网站可以将IP地址映射到位置，其中一个是 www.iplocation.net。当您知道该人之前已连接的WI-FI接入点时—使用 wigle.net 对其进行映射并在 Google 地球上进行更详细的研究。

图

如果您有图片并想知道它的使用位置或首次出现的时间，使用反向图片查找即可。

此外，TinEye 的算法设计与 Google 不同，因此可以返回不同的结果。

为什么有用？作为一名调查员，您可能会需要通过头像找到这个人，因为人们通常不会为他们使用的各种社交网络更改个人资料图片；作为记者，您可以执行与过滤配对的图像搜索以揭露虚假新闻。

如果您需要在社交网络上进行狭窄的搜索，可以使用针对 Vkontakte 的 Findclone 和 Findmevk.com 或者针对 Reddit 的 karmadecay 进行搜索。

此外，值得一提的是浏览器扩展：适用于 Chrome 的 RevEye 和适用于 Firefox 的“图像搜索”选项。

像 CamFind for iOS 这样的移动应用可能会帮助您搜索物理世界中的内容。此外，还有一个 Image Identification Project，用AI识别图像

上的内容。

图像本身包含许多有用的信息，如相机信息、地理坐标等等 —— 它被称为EXIF数据，如果没有删除，您可能会从中发现很多有趣的信息。

例如，映射地理坐标以找出拍摄照片的位置或获取相机序列号，有一项特殊服务：stolencamerafinder.com。

图像编辑工具允许查看元数据，如果您不想要安装复杂程序，跨平台免费软件 Exiftool 可能比较适合您。

第三种方法是在线查看 EXIF 数据：exifdata.com 或 viewexifdata.com。要删除EXIF数据，您可以使用本地安装的工具：exifpurge.com 或在线进行：verexif.com。

您是否需要执行图像取证并查明图像是否被篡改过？使用 Forensically 或 FotoForensics 这些在线工具即可。如果您不想在线上传图片—可以在本地运行 Phoenix 或 Ghiro。

后者更自动化，并提供比上述在线工具更多的功能。

除此之外，使用图像可能需要对其进行去模糊处理以提高质量，因此这里有一些增强工具：

- Smartdeblur—有助于恢复焦点并进行图像改进，从而提供惊人的效果。
- Blurity—仅关注去模糊化，不提供像以前的工具那样的许多选项，仅在Mac上可用。
- Letsenhance.io—使用AI在线增强和升级图像。

[image]

SOCMINT

SOCMINT 是 OSINT 的一个子集，专注于社交媒体平台上的数据收集和监控。

以下是更多的工具。

- ExractFace—从 Facebook 提取数据，使其可脱机使用以作为证据或执行高级离线分析。
- Facebook Sleep Stats—根据用户的在线/离线状态估算睡眠模式。
- lookup-id.com—帮助您找到个人资料或群组的 Facebook ID。

Twitter：

- Twitter advanced search—正如其名；
- TweetDeck—为您提供一个仪表板，显示您的Twitter帐户中的单独活动。例如，您可能会在主屏幕上的某个位置看到针对您的主页Feed、通知、直接消息、和活动的单独列。
- Trendsmap—向您展示来自世界各地的 Twitter 上最受欢迎的趋势、主题标签和关键字。
- Foller—为您提供有关任何公共 Twitter 个人资料的丰富信息（个人资料公开信息，推文和粉丝数量，主题，标签，提及等）。

- Socialbearing—免费的 Twitter 分析，搜索推文、时间表和推特地图。通过参与、影响力、位置、情感等线索来查找、过滤和排序推文或人。

- Tinfoleak—显示了Twitter用户使用的设备、操作系统、应用程序和社交网络。此外，它还显示了地点和地理位置坐标，以生成所访问位置的跟踪地图。在Google地球中映射用户推文等功能。

LinkedIn：

- InSpy—用 Python 编写的。可用于搜索特定组织的员工。此外，它还可以找出组织使用的技术，这是通过特定关键字爬出来的。

- LinkedInt—刮取所选组织中员工的电子邮件地址。支持给定公司域名的自动电子邮件前缀检测。

- ScrapedIn一个 Python 脚本，用于抓取配置文件数据并将其导入XLSX文件（旨在与Google Spreadsheets一起使用）。

[image]

自动化开源情报

互联网是数据的海洋，手动查找信息可能既费时又无效，而且自动化工具可以实现肉眼不会发现的相关性。

这一切都取决于具体情况，是否需要使用这些工具，因为多数工具都需要学习，需要解决复杂问题。

因此，如果您只想完成几个简单的任务，前面提到的东西就已经足够了。

以下是更好的工具。

SpiderFoot ——

如果你想自动化OSINT，它是最好的侦察工具之一，因为它可以用来同时查询100多个公共数据源，它的模块化允许微调查询源。

有四种不同的用例：获取目标的所有内容，了解目标暴露在互联网上的内容，查询黑名单和其他来源以检查目标的恶意与否，通过不同的开源渠道收集情报。最后一个是被动侦察的理想选择。

theHarvester ——

这是一个非常简单但有效的工具，用于在信息收集阶段获取有关目标的有价值信息。

对于被动侦察，theHarvester 使用许多资源来获取Bing、百度、雅虎和谷歌搜索引擎等平台的数据，以及 LinkedIn、Twitter 和 Google Plus 等社交网络数据。

对于主动侦察，它执行DNS反向查找、DNS TDL扩展和DNS暴力破解。

Recon-ng ——

这是另一个很棒的命令行工具，用于彻底、快速地进行信息收集。

这个功能齐全的Web侦察框架包括一系列用于被动侦察、便利功能、和交互式帮助的模块，可指导您如何正确使用它。

对于那些熟悉 Metasploit 的人来说，Recon-ng 会更容易学习，因为

它们具有相似的使用模式。

如果您正在寻找能够快速检查公司在互联网上的可见性的强大功能 —— 这是一个可行的工具。

Maltego ——

这是一个为分析复杂环境而开发的高级平台。

除了数据挖掘之外，它还可以进行数据关联并直观地呈现数据。

Maltego 与您连接的实体（人员，公司，网站，文档等）合作，以便从不同来源收集有关它们的更多信息，以获得有意义的结果。

该工具的独特之处在于“transforms”—一个插件库，可帮助运行与外部应用程序不同类型的测试和数据集成。

FOCA ——

这是一种从分析的文档中提取隐藏信息和元数据的工具。

分析所有文档并提取元数据后，它会进行自动元数据分析，以确定哪些文档是由同一用户创建的。

最新版本仅适用于 Windows。

Metagoofil ——

也是一个命令行工具。对网站下载的公共文档进行分析和元数据提取。适用于 pdf，doc，xls，ppt 和其他格式。

总结

在后隐私世界中保持私密权并控制在这个数字海洋中漂浮的信息是很困难的。

虽然你无法控制关于你的一切，但至少要了解它，这非常重要。

不言而喻，在数字时代，信息起着关键作用，因此那些知道如何找到信息的人将始终领先一步。

这就是本文的目的，以展示🔍开源情报 如何帮助解决广泛的问题：从深度调查到隐私人身安全。

文章中介绍的大部分技巧都很简单，但是会非常强大。因此，如果被用于恶意目的就会造成严重的损害，因此希望您能合理使用它们。

[image]
[image]

如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？

[image] 关键词	个人 反取证 威胁模型 移动设备 防御 预防性
[image] 关联	[image]计算机和移动设备取证；[image]数字技术限制和最佳实践
[image] 创建时间	2019年10月18日
[image] **Description**	操作安全性

手机丢了或者被警察抢走了，这是无比糟糕的事。而且这种危险随时可能发生。为了将损失降至最低，您需要提前作好防备。

- Table of Contents

  提示一：设置生物识别身份验证
  提示二：了解如何快速禁用生物识别技术
  2.1 快速禁用面部**ID**
  2.2 快速禁用指纹**ID**
  总结一下让生物识别快速失效的几种可能性：
  提示**3**：更强的密码
  提示**4**：尽可能快地更新到最新的**iOS**版本
  提示**5**：备份数据
  提示**6**：在锁定屏幕上禁用**USB**附件
  提示**7**：关闭锁定屏幕消息回复
  提示**8**：将**iPhone**设置为自动擦除
  提示**9**：设置查找我的 **iPhone**

[image]

如今我们的电话已经不仅仅是一个电话，说它是身家性命都不为过。您一定理解这个道理。

手机是警方当局和犯罪分子瞄准的重点目标。

为了防止这种情况发生，你应该采取预防措施，越早越好。

提前声明，以下步骤的适用范围不包含您的对手是NSO那类公司的客户时的状况。一般情况下您也很难遇到那种状况（至少他们的间谍工具非常贵，并非随便哪个小偷和警察部门就能买得起的）

以下是一些步骤，是您最基本要做到的。

提示一：设置生物识别身份验证

请注意，这是防小偷的，有可能不防警察（防警察的办法后面说）尤其是在警方可以强迫按压您的手指解锁和/或扫描你的面部而不受惩罚的国家。

您也许曾被建议设置指纹而不是面部ID；因为面部识别可以在不接触的情况下解锁，似乎更不安全。

但是这不确定。

由于禁用很容易，于是，这需要您根据自己面对的实际风险作出尽可能准确的评估。

是的，您的密码依旧是一层安全保护，对某些人而言可能已经足够了，但是 Touch ID 可以增强您的安全性并使窃贼和黑客更难进入您的物理设备。

下一步更最重要。

[image]

提示二：了解如何快速禁用生物识别技术

现在您已经设置了面部ID或触控ID，这是一件非常重要的事：如果抢劫者或执法部门拿走您的 iPhone，它们可能会被用来对付您。

犯罪分子和警察当局可以强行使用脸部或指纹解锁你的 iPhone，后者甚至还有权在合法的情况下没收你的设备。

请注意，掌握时机是非常重要的！

只要知道如何操作，您就可以在瞬间让 Face ID 或 Touch ID 失效，而不会弄乱屏幕上的任何内容。

只需按一下按钮即可锁定生物识别访问。

2.1 快速禁用面部ID

要禁用面部ID，只需同时按住侧面按钮，同时按下开关键音量调高或音量调低按钮。如果你愿意的话，你甚至可以按住所有三个。保持约两秒钟。

一定要保持足够长时间；您需要能看到“滑动关机”开关出现。一旦出现该屏幕，就放手。

[image]

重要提示：如果您的脸部在按下按钮组合之前已经解锁屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，则必须单击侧面按钮一次以关闭屏幕或让它自己睡着。如果不这样做警方依然可以访问您的手机，因为它目前已经解锁。

第二个选项。

连续5次单击侧面按钮（也称为睡眠/唤醒（电源）按钮）将激活紧急SOS屏幕，这将禁用 Touch ID，直到输入密码为止。

使用 iPhone X，X S，X S Max和X R，快速单击Side按钮五次也将激活紧急SOS；它会直接进入倒计时模式，而不是“滑动关机”，所以你必须手动阻止它调用911。但是这样做将有效地禁用 Face ID。

[image]

重要提示：和前面的选项一样，如果您的脸部在执行五次点击之前已经解锁了屏幕，或者您已经在主屏幕或应用程序中处于解锁状态，那么您必须单击侧面按钮一次以关闭屏幕或让它自己入睡，否则无效。

如果您不喜欢这种方法，或者您害怕可能不小心拨打了911，可以在“设置”应用中禁用这一快捷方式。

此外还有一个选项，在上述两个选项都不合适您的情况下。

也就是制造*多次识别失败*和关闭或重新启动设备。

如果您只想暂时禁用 Face ID ，关闭并重新启动 iPhone X，X S，X S Max和X R的方法就有点过了，因为您必须执行与选项1相同的操作，而且要步骤更多。

警告：注意力检测功能是 iPhone X，X S，X S Max和X R的设置，可防止脸部ID在您直接面对iPhone之前解锁iPhone。

设置需要您的全脸—包括眼睛—以解锁您的设备。也就是说，角度是自然的 时就能解锁。但是这个角度很有限。

如果没有激活此注意力检测功能，有人可能会在您不看屏幕时（甚至在您睡觉时）将 iPhone 指向您的脸部来解锁 iPhone。

2.2 快速禁用指纹ID

在美国，执法部门可以让您通过指纹解锁智能手机，但他们不能强迫您输入密码或PIN，这将违反您的第五修正案权利。

在中国，没有第五修正案，他们什么都可以做。所以您需要能快速禁用指纹解锁，并且尽可能争取10次密码 错误以自动擦除手机。

iOS 11及以上都可以做到让您在几秒钟内禁用Touch ID。

想要暂时禁用Touch ID，你只需快速按下电源按钮五次即可，这时屏幕会显示“紧急SOS”页面，你可以呼叫紧急联系人，但同时，这样也可以防止你的iPhone在没有密码的情况下被解锁，也就是说此时已无法用指纹解锁设备。

[image]

如上所示，弹出紧急SOS屏幕，您无需再进行任何操作，只需点击“取消”即可。

在警察砸门之前几秒钟内就可以完成。

下次您尝试使用带有Touch ID的已注册指纹时，它会告诉您“您的密码是启用Touch ID所必需的”。大多数执法部门都无法绕开它。

总结一下让生物识别快速失效的几种可能性：

- 设备刚刚打开或重新启动。
- 设备处于锁定状态超过48小时。
- 在过去的六天半内没有使用密码解锁过设备，且在过去的 4 小

时内没有通过面容 ID 解锁过设备。

- 设备已收到远程锁定命令。
- 面部匹配尝试失败五次后。
- 在同时按住任一音量按钮和侧边按钮 2 秒钟以关机/发起 SOS 紧急联络之后。
- 如果设备的电池电量低于10%。

如上，牢记它们。根据您当时所处的情况，您可以选择最适合自己的一种，以保全设备和人身安全为基本目标。

提示3：更强的密码

如果您在第一次打开 iPhone 时设置了密码，则可能是四位数或六位数字代码。

尽管具有一百万种六位数代码的可能组合比仅有10,000种的四位数代码的可能组合更安全，但它仍然相当弱。

一台名为 GrayKey 的 iPhone 黑客机器可以在大约11个小时内破解六位数的密码。

如果您想要在 iPhone 上获得最佳安全性，则应切换到自定义字母数字或纯数字密码。

两种类型都允许比通常的密码选项更多的数字/字符。如果你想坚持全数字的模式，将你的密码长度达到10位数就可以给它带来1亿种不同的组合。

[image]

一旦您选择了新密码并将其输入了“设置密码”屏幕，您将被要求确认您的新密码，因此请继续操作。

但是，这时您可能会收到提示，要求您使用新密码从 iPhone 更改 Apple ID 密码。

我们建议您跳过此提示，因为它可能让进入iPhone的小偷和警察更容易访问并接管您的Apple / iCloud帐户。所以点击“取消”。（当然，前提是您的iCloud帐户不在“云上贵州”）

取消此提示意味着您需要使用安全问题或双因素身份验证来确认身份并在需要时更改Apple ID密码。

[image]

提示4：尽可能快地更新到最新的iOS版本

这无需更多解释。

当然这种方法无法躲开0day黑市的威胁。但要知道 Apple 的 0day 是超贵的，一般人买不起。

犯罪分子和警方当局可以很邪恶，但是他们也要有价值衡量；如果您的数据价值100万美元，而解锁您的设备以获得数据需要的工具价值200万美元或更多，他们就会退缩。

提示5：备份数据

危险随时都会发生，而且基本不会让您事先收到什么提示。这就是为什么您应该随时做好防备。

现在您不再需要使用 iTunes 将设备备份到计算机上 —— 您可以直接从 iPhone 进行操作。

在“设置”中点击“iCloud”，然后点击“iCloud Backup”。

启用“iCloud Backup”（如果尚未启用），然后点击“立即备份”以备份您的设备。（再一次：需要您不在“云上贵州”）

如果启用了“iCloud Backup”，则当 iPhone连接到电源并且已连接到Wi-Fi时，将自动备份数据。

提示6：在锁定屏幕上禁用USB附件

iOS中有一个更新的设置，允许您连接到附件而无需解锁设备，虽然这确实简化了过程，但它也可以让您面临潜在的风险。

骇客和警察可以利用此功能绕过您的锁屏密码并进入手机 —— 这就是您应该从锁定屏幕禁用USB附件的原因。

在“设置”中，转到“面部识别码和密码”或“触摸ID和密码”，输入您的密码，然后一直向下滚动。确保“USB附件”旁边的拨动开关关闭（不是绿色）。

[image]

提示7：关闭锁定屏幕消息回复

您应该在锁定屏幕上禁用的另一个功能是“回复消息”。

想象一下，有人偷了你的 iPhone，你收到了一个与你亲近的人发来的短信。然后小偷可能会伪装成你，给他们发短信，并以狡猾的方式询问你的密码。

并且还可以采取其他社交工程攻击。

要防止出现这种情况，只需在“面部识别和密码”或“触摸ID和密码”设置中禁用“回复消息”功能即可。

虽然这样做您自己也无法通过锁定屏幕回复消息，但最好先花点时间解锁您的设备，而不是让您的设备更容易被犯罪分子和警察攻击。

[image]

提示8：将iPhone设置为自动擦除

一个非常幸运的犯罪分子可以猜出你的密码，但你可以让这个过程变得更难。稍微有点难就行。

iOS上的“擦除数据”功能会在10次尝试解锁失败后擦除设备上的所有数据，这使得犯罪分子和警方几乎无法访问您珍贵的数据。

只需确保准备好 iCloud 备份，以便以后您自己仍可以访问它。

再次在“面部识别码和密码”或“触摸ID和密码”设置中，打开“擦除数据”旁边的切换按钮，然后点击“启用”将其激活。

如果您是经常忘记密码的人，即使您启用了面部识别码或触摸ID，也可能不想这样做，因为您有时仍需要密码。所以，请斟酌自己的情况。

[image]

提示9：设置查找我的 iPhone

“查找我的iPhone”不仅会向您显示设备的确切位置，还可以让您远程擦除设备，并在您的设备上留下消息和联系信息锁屏。

要启用“查找我的iPhone”，请在“设置”应用中点击您的姓名，然后点按“iCloud”并向下滚动，直至看到“查找我的iPhone”。

在这里，您可以启用“查找我的iPhone”以及“ 发送最后位置 ”；当电池电量非常低时，它会自动将 iPhone 的位置发送到“查找我的iPhone”。

[image]

好了。就是这样。

再次重申，以上步骤能对付大多数危险情况，但是无法对付国家级骇客和间谍；当然，绝大多数情况下您不会遇到后者。所以，先做好基本安全最重要。

[image]
[image]

如何不暴露手机号、不花钱，实现双因素身份验证？

[image] 关键词	2FA 手机号
[image] 关联	[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03 ；[image]匿名手机 ；[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则 ；[image]如果您的手机被盗了或被警察抢走了，怎么办
[image] 创建时间	2019年10月23日
[image] **Description**	操作安全性

比较一下所有可能的选项。

- Table of Contents

  比较图表
  关键比较点
  如何选择这些应用程序
  第一个：**Authy**
  第二个：**LastPass Authenticator**
  第三个：**Duo Mobile**
  第四：**Microsoft Authenticator**
  第五：**Google Authenticator**
  结论

[image]

谈到网络安全，一层是不够的。

复杂的密码（或使用密码管理器创建的密码）可以很好地保护您的数据，但它仍然可以被破解。 [image]什么是凭据填充攻击？如何选择密码管理器？

双因素身份验证通过添加第二层安全性来加强这一点，为您提供更多针对在线威胁的保护。

使用双因素身份验证（也称为两步验证或简称为2FA），您登录的服务需要两件事来验证您：您知道的东西和您拥有的东西。

您的密码用作“您知道的东西”，2FA应用程序提供“您拥有的东西”。

虽然这第二层并非万无一失，但它确实可以大大提高你的防御能力。

并非所有网站都支持此功能，但大多数热门网站都支持此功能，如果感兴趣的话您可以使用 Two Factor Auth 来检查兼容性。

但是，并非所有2FA都是相同的。有些网站仅支持通过短信或电子邮件发送代码。这些是不安全的选项，因为有人可以远程访问这些途径。

这就是为什么说更好的选择是使用基于软件的令牌，这就是本列表中每个应用程序支持的方法。

比较图表

[image]

关键比较点

- 离线模式：无需互联网即可生成2FA代码。

- 开源：源代码可供任何人审核。虽然开源确实提供了优势，但本列表中的应用程序都不是开源的（尽管有些应用程序利用了几种开源技术）。

- 加密备份：令牌数据库已加密，并与您的设备分开备份。这样，即便您升级手机，也无需将新手机注册到所有帐户。

- 桌面版：服务是否具有桌面版本，因此您在登录帐户时不需要智能手机。

- Smartwatch 兼容：该服务支持一个（或多个）主要智能手表操作系统。 Wear OS 是基于 Android 的智能手表操作系统，而 watchOS 则是基于iOS的智能手表操作系统。如果应用程序支持其中一个操作系统，即使手机放在口袋中，您也可以检索代码。

- 密码保护：使用某种形式的身份验证锁定入侵者的能力。Authy 和 LastPass 都支持PIN码，指纹扫描，Touch ID 或 Face ID（取决于您使用的iPhone型号）。

- 多设备同步：能够跨多个设备同步数据并访问您的令牌。在一台设备上添加或删除的任何帐户也将在其他设备上添加或删除。

- 可调节的OTP时间：能够调整一次性密码可用性的长度。较短的时间使黑客更难操作，但可能太不方便。通常默认计时器在15–30秒之间。对于支持该功能的两个应用程序，都需要手动输入。

- 可调整密码长度：可以调整一次性密码的大小。对于支持该功能的两个应用程序都需要手动输入。更长的代码使得攻击变得更加困难。

- 推送通知：列表中的某些应用程序不支持输入代码，而是支持

推送通知。令牌在后台交换而不需要您复制数字，因此您需要做的就是接受或拒绝请求。但是，该网站必须包含支持，仅限于本列表中的所有应用。

- 安全通知：只要对与2FA应用相关联的帐户进行了任何更改，就可以发送提醒。 Microsoft Authenticator 去年推出了此功能，如果您的帐户发生任何更改（例如密码更改），应用程序会通知您。

如何选择这些应用程序

为了缩小 iOS App Store 和 Google Play 商店中2FA应用的范围，本指南设定了一些基本规则。

没有必要为 Android 和 iOS 制作单独的列表。支持这两种操作系统的应用程序将使更多用户受益，因为您可能正在使用这两种移动平台之一（尽管还有 SailfishOS 和技术上的 Windows Phone 用户）。

不幸的是，这个决定确实遗漏了一些很好的选择，包括开源的 andOTP，仅限于 Android。

第二个要求是每个应用程序当前必须由其开发人员支持。

定期支持可确保及时处理错误和漏洞，并且可以及时处理移动操作系统的任何新更新。

本指南删除了至少一年内未收到更新的所有应用程序。例如，FreeOTP 被排除在考虑范围之外，因为其上一次 Android 更新是在2016年，而iOS更新是在2014年。

由于大多数人不想为应用付费，因此本指南只关注免费的2FA应用。

列表中的每个应用都支持基于时间的一次性密码算法，这是基于软件的令牌2FA的首选方法。

第一个：Authy

- **Install Authy: Android (free) | iOS (free)**

[image]

Authy最好的功能是加密备份。无论何时切换手机，只需要在新手机上打开 Authy 并输入电话号码。

然后，你会看到多个连接帐户的选项，包括短信、电话和电子邮件。这些都不够好 。最好的办法是自己的设备。

旧手机上出现提示，输入指定的短语后，您的令牌就可以转移到新设备上了。

但是，如前所述，备份是加密的。因此，您还需要一个单独的密码。

此外，您可以限制哪些设备可以访问您的令牌。

为了最大限度地提高安全性，在设置新手机后，您应该关闭“多设备”选项，这样可以阻止令牌在设备之间同步。

关闭此功能后，即使有人使用其他方法访问您的帐户，他们也无法收到该令牌。

此外，即使禁用了多设备，您仍然可以在多台设备（如平板电脑或计算机）上访问数据库。

如果要移除辅助设备的访问权限，只需选择“允许多设备”下的设备选项，然后选择“删除设备”。

[image]

Authy 还会考虑您的安全性。无论 2FA 应用程序如何改善您的帐户安全性，如果它们本身很容易被击败，那么安全性改进就没用了。

使用 Authy，您可以防范网络钓鱼、恶意软件、暴力密码破解、和中间人攻击。

对 Authy 唯一的抱怨是如何标记设备。

当与多个设备共享数据库时，Android 手机被列为“Android”，因此无法辨别哪个是哪个。但是，iPhone 和PC很容易根据其指定的名称进行标记。

Authy 很容易成为两种操作系统上最好的双因素身份验证应用程序之一。

界面易于使用，您可以安全地转移令牌。您甚至可以更改主页面的布局以便于导航。

第二个：LastPass Authenticator

LastPass Authenticator 在其功能列表中与 Authy 几乎完全相同。两者都提供加密备份，多设备同步和支持推送通知。

但是它缺乏对智能手表和桌面等辅助设备的支持。

- **Install LastPass Authenticator: Android (free) | iOS (free)**

[image]

就像 Authy 一样，LastPass 支持加密备份。唯一需要注意的是，它需要一个 LastPass 帐户，该帐户通常用于存储在线密码。

虽然这不是什么大问题，但您可能会觉得被迫使用您不希望首先使用的密码管理器很烦人。

但更奇怪的是，这两个应用程序是彼此分开的。

无法从密码管理器访问身份验证器，反之亦然，因此，虽然两个应用程序共享同一帐户，但没有其他连接。

话虽这么说，但 LastPass 确实是两个平台上最好的密码管理器，所以如果你没有密码管理器，这是个一举两得的好方法。

LastPass Authenticator 对 Authy 的最大优势是能够调整令牌的参数。

虽然它需要您手动输入代码（而不是扫描QR代码），但您可以修改代码可用的持续时间和代码本身的长度。根据您对安全性或便利性的需求，此功能可能是有益的。

[image]

但是，虽然此功能很有用，但一般公众可能不会使用它。

它是本列表中唯一没有桌面版的。也是本列表中唯一不支持智能手表的应用程序。

无论您是想要 Authy 还是 LastPass Authenticator，安全性都没什么不同。

第三个：**Duo Mobile**

Duo Mobile 专为企业设计，提供适合多个用户的多种计划。

Duo 是一个管理多用户访问和身份验证的安全平台。也是一个优秀的2FA应用程序，设计良好，易于使用。

- **Install Duo Mobile: Android (free) | iOS (free)**

[image]

除了支持 Google Authenticator 支持的相同服务外，Duo Mobile（以及 Authy）还可以更好地支持第三方服务和社交媒体网站。 更新及时。

它支持 Apple Watch 用户使用 watchOS 的官方应用程序。它有 Windows 和 macOS 的官方应用程序，因此从桌面（或笔记本电脑）登录时不需要手机。

它还支持加密的备份。您正在使用的设备将确定备份的存储位置。对于iOS，备份存储在 iCloud 上。对于 Android，备份存储在 Google 云端硬盘上。

[image]

虽然 Duo Mobile 无法同步您的帐户，但能够备份数据库非常有用，因为您决定升级手机时无需重新开始。

第四：Microsoft Authenticator

与 Google Authenticator 类似，Microsoft Authenticator 也不执行云备份。但是与 Google 不同，它受到更好的支持并提供推送通知。

但是后者确实要求用户进入 Microsoft 生态系统。

- **Install Microsoft Authenticator: Android (free) | iOS (free)**

[image]

Microsoft Authenticator 的一个更好的功能是它支持推送通知。

只要您使用该应用程序对 Microsoft 或 Azure Active Directory 帐户进行身份验证，您就会收到一条通知，要求您批准或拒绝发送到您设备的令牌，而不必输入代码。

如果您设备上的令牌与您在登录屏幕上看到的令牌相同，请选择“已批准”。

该过程比输入代码容易得多，虽然其他三个应用程序确实支持该功能，但支持它的服务数量仍有限。

还有安全通知功能。只要您的某个帐户发生重要事件，此功能就会向您的手机发送提醒。

这包括更改密码、从新设备登录、或从新位置登录。这样，您可以立即意识到是否发生了未经授权的操作，并且可以采取正确的操作过程。

[image]

第五：Google Authenticator

有人使用 Google 身份验证器而不是本列表中的其他应用程序有两个主要原因：(可以说）更好的安全性和广泛的可用性。

虽然它相比列表中其他选项具有更多的局限性。但是依旧有很多人在使用 Google Authenticator。

- **Install Google Authenticator: Android (free) | iOS (free)**

[image]

由于 Google 身份验证器不会备份您的数据库，因此数据只存在于您

的设备上。因此，无论何时升级手机，都必须重新连接到所有帐户。

当然这样会更安全。

如果您的设备被盗，现代智能手机可让您远程擦除数据，无论您使用的是 Authy 还是 Google 身份验证器，都可以保护您的令牌。

但是，Authy 将数据库与您的电话号码联系起来，这可能很容易获得也可能被欺骗。

如果有人控制了您的电话线并猜测了您的密码（这是一个很大的问题），他们就可以完全访问您的令牌。使用 Google 身份验证器的话这是不可能的。

Google 身份验证器也是通过应用程序进行双因素身份验证的标准。但是，似乎谷歌正在慢慢放弃该应用程序。更新迟缓。

[image]

Google 身份验证器仅限于桌面用户的 Chrome 扩展程序。

虽然它确实限制用户只能使用 Google 的浏览器，但它可以在所有桌面平台上访问，包括 Chrome OS，与本列表中的其他应用程序不同。它也是本列表中唯一正式支持 Wear OS（以前称为 Android Wear）的2FA应用程序。

老实说，选择 Google 身份验证器的主要原因是您担心将数据备份到云端不安全。

但是，对于大多数用户来说，有更好的选择。

结论

每个人都应该使用2FA。我们知道这很费时，特别是对于不支持应用程序的网站，不得不通过电话号码接收代码不仅不安全也不方便。

使用短信或电话不如专用应用程序更安全，因为您的电话号码很容易被欺骗，允许攻击者远程访问您的帐户。使用基于软件的令牌是更好的方法。

目前 2FA 的最佳选择显然是 Authy。它易于使用，易于转移到新设备，并提供密码保护。

或者，如果您已经是 LastPass 密码管理器用户，并且不介意将您的密码和2FA令牌信任给同一家公司，那么 LastPass Authenticator 可以作为次要选择。

[image]
[image]

如何保持 Android 设备免受警察的侵害

[image] 关键词	威胁响应 移动设备 自卫 预防性
[image] 关联	[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？
[image] 创建时间	2019年10月31日
[image] Description	操作安全性

日常保健可以预防大病。

- Table of Contents

提示**1**：在几秒钟内禁用生物识别
提示**2**：使用强密码
提示**3**：禁用智能锁
提示**4**：隐藏通知
提示**5**：保持您的引导加载程序锁定状态
提示**6**：使用 **Cerberus**
第一步：安装 Cerberus
第二步：授予权限和创建帐户
第三步：将 Cerberus 转换为系统应用程序
方法1：使用 Link2SD
方法2：使用启用 Root 的文件浏览器
第四步：删除Root访问权限
最后

[image]

我们希望从未发生过这种事。但是，执法部门确实会毫无规则地查抄公民的手机，在很多国家都是如此；其中任何数据都有可能令您陷入“自证其罪”的困境。

这种悲剧的发生时间完全无法预测，于是您应该在平时做好基本的防备工作。

本文推荐一些可行的方法，您可以根据自己有可能面对的情况选择最适合的方案，或者将它们结合起来使用。

但我们不是律师，所以请自行判断使用这些方法的风险，因为每种情况都不同，无法全面估测。

提示1：在几秒钟内禁用生物识别

虽然生物识别技术确实在安全性和便利性方面提供了很好的平衡，但是，在遭遇警察的时候，生物识别技术就可能会被用来对付您。

这在美国也一样。虽然最近加利福尼亚州北区地方法院的一项裁决认为警察强迫您用指纹解锁手机违反了第四和第五修正案，这是第一次，但未来的法庭听证会结论如何还有待观察。

在 Android 9 Pie 中，谷歌推出了一项称为锁定模式的功能。默认情况下不启用它，因此您需要手动打开它。

激活后，您可以快速锁定手机，并一键禁用生物识别，将PIN、图案或密码作为解锁手机的唯一方法。

最重要的是，它只会禁用您的指纹扫描仪（或面部识别）一次，因此您不必记得再去关闭该功能。

这是 Android 的一个很好的补充，因为警察、抢劫犯和其他潜在的攻

击者可以强迫你或者用你的指纹、面部或语音来解锁智能手机。或者，具有相似的面部或语音的人可以在没有生物识别签名的情况下解锁您的手机。

但是，在执法方面，由于第5修正案权利，警察无法合法地让您输入密码。

即便对于非美国用户来说，没有第5修正案保护，使用该功能也能保护您免于如上所述的很多危险，至少能在警察面前拖延时间。

此外在 Appl 设备要求您一起按下两个按钮几秒钟以触发其锁定模式（在较新的 iPhone 上）；或连续五次点击一个按钮（在较旧的 iPhone 上）。

要在 Pixel，Pixel XL，Pixel 2 或 Pixel 2 XL 上解锁 Android 9.0 中的这一新安全功能，您只需转到设置中的“安全和位置”即可，然后点击设备安全性下的“锁屏首选项”。

接下来，只需确保切换到“显示锁定选项”，即可完成设置。

[image]

如果您没有看到此选项，可能是因为您选择了滑动屏幕锁定而不是模式、PIN 或密码。

现在，要实际使用锁定模式，只需长按电源按钮，直到电源菜单出现。

您会看到锁定按钮出现，具体取决于运行的 Android Pie 版本。

下次尝试解锁手机时，您需要先输入您的模式、PIN或密码。

如果您的手机运行较旧的 Android 版本，还有另一种解决方法：只需重新启动即可。

当然，不会建议您因为这一便利而拒绝更新。

提示2：使用强密码

在提示1 的前提下，手机提供的最安全的身份验证方法是字母数字组合的长密码。

使用安全密码（最长可达16个字符），您可以放心，未经您的同意，您的手机将无法解锁，因为执法部门即便使用暴力破解也需要很长很长时间的猜测过程。

纯数字（或使用常用词或名字）的8个字符的密码将需要一台计算机超过五个月才能破解；将此值增加到16个字符，破解需要几千年的时间。

这可以是让任何人（包括执法部门）远离您手机的安全选择。

提示3：禁用智能锁

很多人喜欢使用 Android 的智能锁定功能，可以更轻松地解锁自己的设备，但是要知道，这是一把双刃剑：它还可以让警察更轻松地进入您的手机。

特别是“On-Body Detection”设置，当运动传感器检测到自从上次使用PIN、模式或密码解锁后一直在移动时（以与行走者一致的方式），可以保持手机未锁定状态。

这种状态下如果您遇到警察拦路检查，情况就会很糟糕，他们可以通过简单的滑动解锁您的手机。

智能锁的“可信位置”设置也存在风险。这可以让您的手机在家中等特

定位置被自动解锁。

如果警察闯进您的家里，就可以在没有PIN、模式或密码的情况下解锁您的手机。

要禁用所有 Smart Lock 选项，请转至设置 →安全 →智能锁，然后单独选择每个项目并禁用它们。

转至“可信任位置”，删除其中的设置。

提示4：隐藏通知

通知是很糟糕的东西，因为它设想的是永远只有您自己掌握手机，这显然非常不现实。

虽然锁屏确实阻止了警察访问手机内容，但即使无法访问手机的其余部分，自动弹出通知也很可能成为重要信息来源。

这是因为，默认情况下，通知（特别是消息）可以在锁定屏幕上阅读—— 有时甚至是完整的消息。

要更改这种情况，请打开“设置”并选择“安全性和位置”（在不同手机上可能会有不同的标记；搜索 “安全” 很容易找到）。

选择“锁定屏幕首选项”和“锁定屏幕”。从弹出窗口中，选择“隐藏敏感内容”或“根本不显示通知”。

如果您的手机配备了通知 LED，我们建议选择后者，因为它提供了最好的保护。

LED 闪烁您就会知道有新的通知，但它们永远不会出现在锁定屏幕上。

如果没有 LED 建议选择“隐藏敏感内容”。

或者，如果您的手机使用的是 Android 9 或更高版本，则可以使用“锁定模式”选项作为临时禁用所有锁屏通知的方式，以防您被警察骚扰或扣留。

触发锁定模式后，直到您下次使用模式、PIN 或密码解锁设备，通知才会显示在锁定屏幕上。

提示5：保持您的引导加载程序锁定状态

Android 有一个检查和平衡系统，以确保在启动时操作系统的每部分仍然是安全的。但它也是一个开放的操作系统。

为了对希望 root 并同时强化启动安全性的用户保持开放状态，谷歌想出了一个默认情况下锁定 boot chain 的系统，但如果你愿意，你可以使用两部分设置来打开它。

其中一个设置在 Android 操作系统内部，另一个设置在一个名为 bootloader 的预启动菜单上。

Android 内部的设置称为OEM解锁。这里的想法是，如果您输入了模式、PIN 或密码以进入操作系统，才会启用此选项。因此如果它已启用，那么就是由您来启用的。

从 Android 内部启用该设置后，您可以进入引导加载程序模式并发送 Fastboot 命令以解锁引导加载程序。

这将允许您在设备上安装非官方软件，例如自定义恢复或自定义 ROM。反过来，这些可以帮助您获得手机的 root 访问权限。

为了使事情更安全，解锁引导加载程序的实际操作会自动擦除设备上

的所有数据。

但是：如果您的引导程序当前已解锁，执法部门可以轻松地在设备上安装非官方固件，以绕过锁定屏幕并访问您的数据。

OEM解锁设置并不值得担心，因为它只允许解锁引导加载程序。

如果警察确实解锁了您的引导加载程序，您设备上存储的所有数据都将被自动删除。

但是，如果您在启用 OEM 解锁后解锁了引导加载程序 —— 例如，如果您将手机与Magisk一起使用 —— 那么，非常建议在完成后返回并重新锁定引导加载程序。

此外，如果您安装了自定义恢复（如 TWRP），则应确保使用密码保护恢复菜单。

启用“OEM解锁”选项在技术上不太安全。理论上，技术娴熟的小偷可以在启用此选项的情况下完全擦除您的设备，这意味着您将无法再使用 Android 设备管理器跟踪设备的位置。但 Android 的其他安全措施仍然存在，因此没有您的模式、PIN或密码，任何人都无法访问您的数据。

提示6：使用 Cerberus

Cerberus 是Play商店中的第三方应用程序，提供 Google 的查找我的设备等所有功能。

虽然它确实有订阅费用，但它是一个比查找我的设备更完整的安全软件。

一个重要的补充是：它能够向手机发送命令以远程控制它。

- https://www.cerberusapp.com/home/zh

在警方拿走您的电话的情况下，Cerberus 允许您发送短信或使用浏览器向您的手机发送命令。

一个命令即可使用您选择的代码锁定手机，该代码与锁屏代码相区别。

此外如果您判断后认为手机再也拿不回来了，则可以使用SMS命令（或通过浏览器）远程擦除手机。

这样，即使警察绕过任何其他保护性方法，手机上也没有任何东西可供他们检索。

但是，请确保删除备份，如 Android Pie 之前，这些文件是未加密的，登录到您的 Google 帐户的任何人都可以访问这些文件。

送一个短片给大家，荷兰电影制片人 Anthony Van der Meer 的作品，自发表后迅速成为了热门。

该视频包含很多在设备被盗后远程拍摄的屏幕截图、音频剪辑和录像。

Van der Meer 使用就是 Cerberus。

下面简单介绍一下它怎么用。

第一步：安装 Cerberus

首先，您需要安装 Cerberus。安装过程将非常普通。

[image]

第二步：授予权限和创建帐户

按照屏幕上的提示确保 Cerberus 具有所需的所有权限，然后系统会要求您创建一个帐户。

完成后，您将立即开始为期7天的免费试用。如果您希望在此之后继续使用 Cerberus，则需要以每年5.00欧元（约合5.23美元）的价格订阅。

[image]

第三步：将 **Cerberus** 转换为系统应用程序

这一步骤可以让小偷从你的手机上移除 **Cerberus** 几乎不可能，并且反过来又可以让你无限期地追踪你的手机。

这里唯一需要注意的是，手机仍然需要联网才能完全跟踪，但除此之外，即使小偷在您的设备上执行恢复出厂设置，安全软件也会保持活动状态。

您可以使用两种方法来完成此部分。

方法1：使用 **Link2SD**

- https://play.google.com/store/apps/details?id=com.buak.Link2SD

之后，只需打开该应用程序，然后点击超级用户访问请求中的“授予”。

从这里，找到并长按 Cerberus 条目，然后从弹出窗口中选择“转换为系统应用程序”。

[image]

方法2：使用启用 **Root** 的文件浏览器

只需从设备的根分区前往/ data / app文件夹，然后找到并复制 com.lsdroid.cerberus 文件夹。

接下来，前往/ system / app文件夹，然后将 Cerberus 文件夹粘贴到此位置。

[image]

接下来，长按新复制的文件夹，然后从菜单中选择“权限”。

之后，设置权限，如下面的第二个屏幕截图所示。

如果您的文件浏览器有选项可以复制子文件夹和文件的这些权限，请确保勾选。

否则，对 Cerberus 文件夹内的任何子文件夹使用相同的权限设置重复此相同的过程。

[image]

完成后，只需重新启动手机，Cerberus 将作为系统应用程序安装。

第四步：删除**Root**访问权限

既然 Cerberus 已作为系统应用程序安装，则无法使用传统方法或出厂重置设备来卸载它。

这是很好的防盗功能，因为该软件几乎可以在设备开机并连接到互联网的任何环境中保持活动状态。

但是，如果你的手机被一个精通技术的小偷或警察偷走，他们可以使用像 Titanium Backup 这样的 root 应用来卸载 Cerberus。

或者，他们可以在第一时间使用您使用的相同root访问权限撤消刚刚进行的更改。

所以，建议打开你的 SuperSU 应用程序，前往 Settings 选项卡，然后点击“Full unroot”按钮。

只要重新启动你的手机，Cerberus 将成为一个永久性的固定装置。就像 Van der Meer 在视频中所做的那样。

[image]

最后

前面的提示方法比较基础，希望能使用在日常中成为习惯；最后一个方法也许比较适合中国的安卓用户，比如传说中在街头强行检查手机的情况。

[image]
[image]

攻击加密系统的多种形式和防御方法

[image] 关键词	2FA 加密 对抗性思考方式 隐写术
[image] 关联	[image]一次性密码和2FA应用 ；[image]如何使用社交工程来攻击 2FA？ ；[image]开源 2FA 应用 ；加密
[image] 创建时间	2019年11月19日
[image] **Description**	操作安全性

全盘加密不是万能的，但的确是应该被推荐的。

- Table of Contents

  对加密系统的常见攻击方式有三种：
  对加密系统的攻击
  加密攻击的对策
  1、硬件攻击（如恶意女仆等）依赖于攻击者获取受害者机器访问权限的能力；所以你应该：
  最后

[image]
[image]

激进社区用户请从这里进入：加密

许多人认为密码学和加密这两个术语是可以互换的，但并不完全正确。密码学是“秘密写作”的科学，它的用法有着非常悠久的历史，而且多年来它已经出现了多种形式。密码学有两个主要组成部分，加密

和隐写术。

在加密中，人们加扰数据使其无法被直接读取。它使用算法和密钥将明文转换为加密文本（也称为密文）。这可以保护您的数据免遭未经授权的访问或潜在的攻击者。

隐写术则是在普通信息中隐藏秘密信息的科学，因此在传输过程中保持其秘密。

[image]

可在本站“🔲工具-Tools ”专栏中搜索“隐写”，以找到相应的工具。

隐写术可以与加密相结合，以进一步保护传输的数据；现代的隐写工具实现了这种方法。

加密被认为是信息技术系统任何安全性的主要组成部分，因为它提供了信息安全的最基本的四种服务：身份验证、不可否认性、机密性、完整性。

加密有助于人们在静态和跨越不受信任的媒介（如互联网）时保持数据的安全性。

加密数据永远不会是满足我们所有安全需求的100%解决方案。

技术不断发展，以产生更安全的加密系统/算法，与此同时攻击者的技术能力也在增强。

对加密系统的常见攻击方式有三种：

1. 窃取加密密钥（例如 Brute Force 和 keyloggers）

1. 密码分析（攻击加密算法本身）

1. 攻击实现加密算法的软件程序，

绕过今天的加密系统最常用的方法是窃取用于解密数据的密钥，这将是本文中的重点。

本文分为两部分：第一部分讨论针对全盘加密（以及其他一般加密方法）的攻击；第二部分讨论减轻此类攻击的对策技术。

[image]

对加密系统的攻击

最著名的针对加密系统的攻击包括但不限于以下形式：

- 恶意女仆攻击 **[image]** 恶意女仆和查抄

这种类型的攻击需要物理访问受害者的计算机，攻击者将一个恶意引导加载程序安装到系统上。

下一次受害者启动计算机时，他将从被骇客入侵的引导加载程序启动，受害者需要输入解密密钥/密码来解密计算机驱动器（假设受害者计算机使用了全盘加密保护），被入侵的引导加载程序将捕获受害者凭证供以后检索。

可信平台模块 TPM 可以检测对原始引导加载程序的任何修改，并在此情况下阻止计算机启动。

什么是可信平台模块（***TPM***）？

TPM 是位于计算机主板上的小型微芯片。大多数现代 Windows 设备都配备了这个芯片；一些主板制造商允许单独添加该芯片。

TPM 在全盘加密方面的主要作用是存储加密密钥。它还提供了一种机制来检测任何更改主机操作系统软件的尝试（例如 Bootkit 攻击）或攻击者用来破解加密驱动器的硬件。

一旦TPM检测到任何更改，它将使您的PC以受限模式启动，从而防止攻击者从您那里获取任何可以帮助他们破解加密驱动器的信息。

- **Bootkit** 和 **Rootkit** 攻击

Bootkit 是一种 BIOS 级别的攻击，它通过将恶意软件隐藏为主引导记录（MBR）或卷引导记录（VBR），然后在操作系统启动之前执行此恶意软件。

由于MBR无法加密，这种攻击的危害可能超过FDE。Bootkit 恶意软件可以直接访问 Windows 内核，使其可以不受限制地访问所有 Windows 功能。

检测 Bootkit 非常困难，因为它的代码驻留在OS文件系统区域之外，常规防毒软件无法检测到它。

一些软件声称能够删除著名的 Bootkits，但是，删除已感染 OS MBR 的 Bootkit 可能会同时删除重要启动文件导致操作系统无法运行。

另一方面，Rootkit 也是一种试图获得对您的计算机的管理访问权的恶意软件。

Rootkit 通常通过扫描操作系统以查找可能存在的漏洞（例如未修补的 Windows），然后尝试利用其中一个漏洞悄悄访问系统。

Rootkit 可以在他/她不知情的情况下监视受害者计算机上的所有内容。

检测 rootkit 有点困难，其中有些家伙使用多态技术重写其核心引擎

代码（更改其代码签名）以防止专门的反 rootkit 软件检测到它。

Bootkits 和 rootkit 都是一种键盘记录程序，可以记录您在计算机上键入的所有内容（例如加密密钥和密码），然后将数据传输给其运营商。

在大多数情况下，只有通过执行操作系统的全新安装才能删除 Rootkit 和 Bootkits；一些高级 Bootkits（例如硬件/固件 Bootkit）需要重新安装 BIOS 或受感染的固件。

- 冷启动攻击

这种类型的攻击发生在攻击者获得物理访问权限的地方，攻击者能够在使用冷启动重新启动计算机后从运行的操作系统中检索加密密钥。

现代移动设备不容易受到传统的冷启动攻击，因为 RAM 内存是直接焊接到主板的。

冷启动攻击的另一种方法是按下PC上的重置按钮（或突然从PC断电）并尝试通过引导到另一个操作系统，提取剩余的数据，包括 RAM 内存中的任何加密密钥/密码。

可以通过加载可引导的 DVD / CD 或可引导的 USB 记忆棒来实现引导到另一个OS。

攻击依赖于 DRAM 和 SRAM 的数据残留特性检索断电后数秒至数分钟内内存中的可读内容。

许多实验表明，DDR3 及更高版本不易受冷启动攻击，因为它们失去电压太快。

尽管使用现代计算机硬件无法成功实现冷启动攻击，但仍然认为它应该被考虑为有效的攻击形式，尤其是当您仍在使用旧硬件PC时。

- 暴力登录攻击

理论上讲，如果时间充足，这种攻击可以解密任何加密数据。

暴力登录攻击通过尝试猜测所有可能的密码/密码短语组合来找到正确的那个。

在全盘加密的情况下，它可以针对预启动身份验证和恢复密钥执行；也可能针对操作系统登录身份验证。

最常见的暴力攻击类型称为字典攻击或混合暴力攻击。这种攻击始于单词词典，因为大多数人会使用易于记忆且不完全随机的密码。

针对此类攻击的最佳对策是使用复杂的长密码，因为密码长度增加时，破解密码所需的时间就会显著增加。

- 直接内存访问

直接内存访问（DMA）是计算机系统的一项功能，它允许某些硬件组件直接与主计算机内存（RAM）交互，并在不使用 CPU 的情况下传输数据。

该技术用于加速处理时间并提高计算机吞吐量，因为数据直接从RAM存储器传输而无需先在CPU中处理。

攻击者可能会利用此功能从目标计算机窃取敏感数据，绕过所有操作系统安全机制以及任何锁屏和防病毒软件。

该方案的工作方式如下：

攻击者将他的设备（笔记本电脑）连接到受害者计算机，该设备有一个特殊的破解软件，破解软件将在受害者 PC RAM 内存中搜索感兴趣

的东西，如加密密钥、密码或解密文件。

攻击者还可以使用这种技术安装后门，完全侵入受害者的机器。

为了使攻击起作用，受害者的PC应该有支持DMA的接口，包括：FireWire，Thunderbolt，PCMCIA，PCI，PCI-X 和 PCI Express。幸运的是，USB 接口不支持DMA。

- 加密勒索软件攻击

这种攻击最近特别流行，它是一种反向全盘加密，攻击者加密受害者文件并要求给钱才能解密。

勒索软件是一种恶意软件，可以感染您的设备，无论是计算机还是智能手机，都可以做到阻止用户对存储数据的合法访问。

这种恶意软件有不同种类，有些类型对于经验丰富的计算机用户来说很容易恢复，但其他类型更危险，通过加密受害者计算机驱动器上的所有数据使其无法访问。

以上就是”最流行的”针对全盘加密的攻击形式。这些攻击也可能发生在操作系统登录身份验证本身或针对可用于加密单个文件或创建加密卷的任何其他加密软件。

第二部分中将介绍如何降低这些风险以防止攻击者未经授权访问机密数据。

[image]

加密攻击的对策

以下措施（如果能正确实施的话）将帮助用户缓解针对其加密数据的大多数攻击。

1、硬件攻击（如恶意女仆等）依赖于攻击者获取受害者机器访问权限的能力；所以你应该：

- 1.1 为 BIOS / UEFI 设置密码，这将防止攻击者修改引导顺序以从USB / CD或DVD驱动器引导以执行恶意操作。

- 1.2 在 PC 启动之前使用预启动身份验证（**PBA**）对用户进行身份验证，这样，用户必须在解锁加密卷和启动 Windows 之前提供某种形式的凭据。通常使用PIN或USB闪存驱动器作为密钥或令牌进行身份验证。

- 1.3 尝试使用统一的可扩展固件接口（UEFI）认证设备。

由于只有 PC 的硬件制造商可以访问创建有效固件签名所需的数字证书，因此 UEFI 可以防止基于固件的 Bootkit。

- 1.4 对于那些不断旅行且需要随身携带敏感文件的人来说，可以通过将启动分区和引导分区安装到便携的USB记忆棒中并随身携带来抵消恶意女佣攻击。

通过这种方式，即使攻击者获得了对目标笔记本电脑的物理访问他也无法破解目标的加密密钥，因为用户将从存储在USB上的引导加载程序启动。

2、安装最新版本的系统，并使其保持最新。当然这种方法无法抵制 NSA —— 斯诺登文件显示，微软把零日给国安局，而不是修补它。

3、禁用 hyberfil.sys 和 Pagefile.sys：hyberfil.sys 负责 Windows 操作系统的休眠模式。

它通常驻留在系统驱动器上，是一个隐藏的操作系统文件。启用休眠模式时，它用于存储 Windows 的当前内存状态。休眠文件通常会存

储加密密钥。

4、DMA 利用PC上的 DMA 端口直接访问计算机RAM内存。为了减轻此类攻击，您可以：

- 4.1 禁用 BIOS 或 UEFI 中的DMA端口。
- 4.2 阻止与此类端口的物理连接来实施物理安全措施。
- 4.3 安装最新版本的系统并使其保持最新。

5、针对冷启动攻击的缓解措施：此攻击已经少见，主要适用于仍使用旧版RAM的计算机。许多研究表明，使用 DDR3 及更高版本的 RAM 比以前的版本安全得多。

6、多重身份验证始终是个好主意。

7、要对抗 Bootkits、Rootkit 和其他恶意软件，请按照下列步骤操作：

- 7.1 在使用防病毒程序扫描电子邮件附件之前，请勿打开电子邮件附件；通过电子邮件发送时，不应打开可执行程序和脚本。
- 7.2 在执行从 Internet 下载的任何软件之前，请务必小心。最好在隔离的虚拟机上执行此类程序，然后再将它们安装到工作PC上。
- 7.3 请勿将任何未知来源的可移动介质（如 USB 记忆棒、DVD、CD、外部硬盘和SD卡）插入计算机。许多病毒都驻留在此类可移动介质上，即使您拥有防病毒软件也会感染计算机。

8、使用长的、随机的和复杂的密码可以减轻攻击。还有双因素身份

验证。 [image]如何不暴露手机号、不花钱，实现双因素身份验证？

反 **Bootkit** 和 **Rootkit** 的工具：

- RootkitRevealer（https://technet.microsoft.com/en-us/sysinternals/bb897445

- TDSSKiller（https://support.kaspersky.com/viruses/disinfection/5350#block1 ）

- GMER（http://www.gmer.net）

- UEFI 的 Rootkit 检测框架（https://www.reversinglabs.com/open-source/rdfu-uefi.html ）

- UnHackMe—30天免费试用（http://greatis.com/unhackme ）

- Sophos Anti-Rootkit（https://sophos-anti-rootkit.en.uptodown.com/windows ）

最后

有一种常见的误解，即加密硬盘会使您的计算机安全，但这并非完全正确。事实上，磁盘加密仅对有物理访问您计算机的攻击者有用。它并不会使您的计算机更难以受到通过网络进行的攻击。

攻击者仍然可以利用社交工程学欺骗您安装恶意软件，您仍然有可能访问了恶意网站，等等无数被入侵的形式。当然，磁盘加密对阻止互联网监控也没有任何作用。政府间谍可以利用构成互联网骨干的光纤电缆，几乎可以监视你在网上做的所有事。需要完全不同的加密类别来解决该系统性问题。

但是现在重要的是要知道磁盘加密可以防止单一攻击：物理访问。

磁盘加密的目标是，如果不是您本人的某个人访问您的计算机，比如抢走设备的警察，他们将无法访问您的任何文件，只会看到乱码，无用的密文。

BitLocker 和 FileVault 只是最懒的解决方案。更好的选择是免费开源程序 VeraCrypt（适用于 Windows，MacOSX，Linux）。它绝对是无价的，特别是如果你使用几个不同的系统并有特定的愿望的话。

[image]
[image]

这些使用暗网的人是如何被抓到的？: 总结教训

[image] 关键词	反侦察 反追踪 暗网
[image] 关联	[image]S04完美隐身-总章节：机智是重要实力 ；[image]使用Tor保护自己时千万不要做这9件事 ；[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2019年12月13日
[image] Description	操作安全性

很多情况下，你只有一次犯错的机会。所以，应该非常小心。

- Table of Contents
Emil Babadjov
总结 **Babadjov** 的低端错误：
Abudullah Almashwali 和 **Chaudhry Farooq**
总结他俩的低端错误：
Jose Robert Porras III
结尾

[image]

如今暗网对当局来说早已不再是深不可测了。他们已经多次成功从暗网抓捕目标人。

本文即将讨论的不是技术问题，而是人的问题 —— 是基本操作安全方面的错误导致的追踪和逮捕。

暗网依旧是活动家和记者躲避当局监控的途径；如果敏感人士犯了类似的错误，任何反追踪技术都会失败。

于是本文认为有必要梳理一下他人的教训，以帮助更多人提高警惕性。

以下是一些比较著名的案例。

Emil Babadjov

（又名 Blime-Sub 和 BTH-Overdose）

Babadjov 的职业生涯相当短暂，并且他犯了一些令人惊讶的低端错误，其中许多错误就是导致他被捕并随后被监禁的原因。

通过 Alphabay 上的 Blime-Sub 和 BTH-Overdose 帐户，Babadjov 出售芬太尼、海洛因和甲基苯丙胺。记录显示，Babadjov 仅在 Alphabay 就完成了近2,000次销售。

2016年1月，缉毒局（DEA）的一个工作组将他的账户确定为破解和逮捕暗网供应商的潜在目标。

根据DEA特工 John Brown 的一份刑事诉讼：多个讨论暗网市场的论坛中用户发布的信息都显示了 Babadjov 运送包裹的大致位置。

客户注意到 Blime-Sub 和 BTH-Overdose 这两个账户都从大约相同的区域运送包裹：西海岸，“可能在加利福尼亚的某个地方”。

[image] *Alphabay* 上的 *Blime-sub* 列表

特工 Rabaut 检查了与 Alphabay 供应商账户 BTH-Overdose 相关的PGP密钥的用户身份信息。

虽然 Babadjov 没有使用他的真实姓名，但他使用了一个致命的电子邮件地址：babadjov@gmail.com。

简单的开源情报收集就让DEA特工找到了登记为 “Lime Vojdabab” 的 Facebook 帐户。

一个假名，而且显然是 Emil Babadjov 倒着拼的结果。这种方法太傻了。

SA Rabaut 向数字货币兑换商 **Coinbase** 发送了传票，要求他们提供有关 babadjov@gmail.com 的任何信息。

Coinbase 提供的数据显示，Emil Babadjov 于2015年11月13日使用相同的电子邮件地址注册了一个帐户。

[image]

DEA特工提交的第二次搜索也取得了积极成果。他以被告的名义搜索了用户信息。

Coinbase 的记录表明，Emil Babadjov 曾试图在2016年3月18日创建一个新的 Coinbase 帐户。

他提供了一个电子邮件地址，将账户 BTH-Overdose（PGP密钥和电子邮件地址的来源）与 Alphabay 供应商帐户 Blime-Sub：blimesub@gmail.com 联系起来了。

调查人员在逮捕前收集到了更多的证据，突出的一个要素是 Babadjov 的身份证明。

执法部门假扮买主，从 BTH-Overdose 账户订购了一揽子药物，邮寄

地址是位于加利福尼亚州旧金山的自助服务亭（SSK）。于是这些间谍与美国邮政检查局合作，追踪了特定的SSK以及某人支付邮资的具体时间。

由于SSK交易不是面对面交易，因此SSK系统会拍摄进行交易的人的照片。

检查员把嫌疑人的照片给了间谍，⚠间谍根据对嫌疑人的加州驾驶执照照片和社交媒体照片的对比，将嫌疑人识别为 Emil Babadjov。

Babadjov 目前正在加利福尼亚州 Lompoc 的低安全性联邦惩教所服刑。

总结 **Babadjov** 的低端错误：

- 致命的电子邮箱 babadjov@gmail.com

千万不要使用与你的真实身份存在任何联系的注册信息（见《完美隐身：技术增值部分》）；千万不要使用谷歌服务（见教训《他们是如何抓捕说真话的人？》）

- 低端的假名

这是最愚蠢的部分，但可以说很多人都会在此犯错 —— 当人们尝试给自己换一个名字时，他们往往非常缺乏创意，因为他们会下意识的感觉“那个名字是不是合适我”。

这是致命的错误！越是“合适你”的名字，说明越容易与你的真实身份发生联系。就像现实中的乔装，你必须选择*非常不合适你*的服饰，正常情况下你永远都不会碰的衣服，那才是最好的乔装。

- 数字货币兑换商和自助服务亭提供的信息

这似乎很难根本性避免，但你完全可以采取我们在“完美隐身”系列中介绍的狡兔三窟游戏，让追踪者撞墙。在这里回顾 [image]令人兴奋的心理过招：完美隐身 S04E06 。

- 更加令人哭笑不得的是社交媒体照片

社交媒体晒照片有多致命就不用说了。如果您曾经在互联网上任何地方发布过自己的照片，并且无法彻底删除，那就请彻底放弃相关身份，彻底分身，否则不要参与任何敏感的对话和行动，⚠否则会连累其他队友。

Abudullah Almashwali 和 Chaudhry Farooq

（又名“Area51” 和 “DarkApollo”）

Almashwali 和 Farooq 在 Alphabay 暗网市场上销售阿片类药物。他们使用供应商帐户 Area51 和 DarkApollo 作为用户名。

不出所料，Babadjov 被捕背后的缉毒局（DEA）工作组也调查了 Almashwali 和 Farooq。

DEA特工 John Babaut 是 Babadjov 案的首席调查员，就是他领导了对 Almashwali 和 Farooq 的调查。他在两次调查中都采用了相同的策略。

或者说，两个案子中的被追踪对象犯有类似的错误 —— 没能完全隔离真实身份。

[image] 来自 *Area51* 的海洛因 *Alphabay* 列表

Alphabay 上的 Area51 和 DarkApollo 供应商帐户的用户ID包含链接到其他服务的电子邮件地址：Adashc3l@gmail.com。

而“其他服务”直接将被告确定为帐户所有者了。

在社交媒体上简单地搜索 “Adashc31”和“Adashc” 就能发现 Twitter、Instagram 和 Facebook 帐户，属于被识别为 Ahmed 的人，名字是 Farooq 或 Ch. Ahmed Farooq，这是写在刑事诉状中的。

[image] *Farooq* 的推特账号

根据来自论坛的有关暗网市场和供应商的信息（可能是/ r / darknetmarkets），特工知道 Area51 和 DarkApollo 的邮寄包裹来自纽约布鲁克林的邮局。

同时与“Adashc31”搜索相关的 **Facebook** 个人资料显示”Farooq”居住在纽约。

SARabaut 传唤了Facebook 以获取与该帐户相关的所有信息。Facebook提供了有关Farooq的信息。

值得注意的是，根据起诉书，间谍收到的电话号码是“针对在纽约布鲁克林销售海洛因的毒品贩运组织（DTO）正在进行的调查的一部分。”

执法部门与 Area51 和 DarkApollo 进行了秘密交易（在起诉书中称为UC Parcels）。这些包裹包含执法部门订购的海洛因以及 **Almashwali** 的指纹。

[image]

邮政检查员发现了Almashwali常用的自助服务亭（SSK）；DEA 特工确认了SSK拍摄的相关照片。

Farooq 的脸似乎避开了监视相机，Almashwali 作为他的托运人，使 Farooq 不受调查人员的影响。

但Almashwali 在支付SSK邮资时使用了 Farooq 的信用卡。该卡与Farooq的真实姓名和地址相关联。

[image]

2017年7月24日，一名联邦法官判处 Almashwali 在监狱服刑6.5年。2018年1月23日，Farooq 被判处入狱23个月。

总结他俩的低端错误：

- 使用真实身份信息标注 Facebook 个人资料是史上最愚蠢的行为

如果你必须使用 Facebook或其他类似巨头服务（对于活动家来说的确如此），可参见：

[image]

返回：[image]社交媒体上的行动主义安全性:框架手册

返回：[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗

- 信用卡是致命之源。信用卡和任何在线支付都是你的完整生活全景图

Jose Robert Porras III

（又名 “Canna_Bars” 和 “TheFastPlug”）

与许多其他供应商一样，**Jose Robert** 栽在将比特币兑换成美元上。

尽管只要有一个错误就足以致命了，但这个错误依旧是相当独特的。

纽约的卧底特工假扮洗钱服务以接近暗网供应商。供应商将比特币和其他加密货币交给洗钱者，以兑换美元（是的，这是真事）。

Porras 和数十家不相关的供应商从联邦特工那里收到了现金，该特工控制了一家由暗网洗钱者经营的账户。

[image] 请注意 *4072 11th Avenue*，*Sacramento California* 地址。

当然，这些信息在 Porras 被捕时就被密封了，而且所有细节—即使在整个行动中被捕的所有供应商都被定罪后—仍然是密封的。

也许其他案例能提醒一些相关的侦查策略，参见 https://iyouport.substack.com/p/vpn?utm_source=publication-search

目前联邦特工很可能继续在暗网操作被扣押的洗钱者帐户。当局随后在 Porras 案中提出了一项替代起诉书，增加了十几个洗钱指控。

[image] 卧底特工拿到的第一个地址

这项调查中最独特的部分来自一张广告照片 —— Porras 在 Canna_Bars 别名下发布的大麻广告。

为了证明大麻的质量，Porras 在大麻的照片共享服务 Imgur 上发布了几张照片。就是下面这样 —— 灾难之源。

[image] *Canna_Bars* 展示他的产品质量的照片

你能看到他居然没有戴手套！ ……一名临时吸毒者也许没有什么可担心的，但是作为供应商，应该明白自己一直在与执法部门进行持续的猫鼠游戏。

供应商非常多，但是被抓住的只有那几个，为什么？因为只有那几个太不擅长匿名了。就如类似 **Porras** 这种低端错误。

2018年3月19日，特工在 Imgur.com 网站上下载了最高分辨率的上述广告照片，并将照片提交给了HSI法医文件实验室，以便与已知指纹进行比较 —— 指纹，逮捕的证据。

[image] *Porras* 的高清指纹

这就如带着面具却摆出剪刀手的拍照效果……

[image]

我们提醒过不要在互联网上晒剪刀手照片。拍照时，如果你在距离摄像头三米内摆出剪刀手的手势，通过照片放大和人工智能增强技术，就能将你的指纹信息还原出来 —— 不仅会导致你的身份被识别，

并且，你家里的指纹锁、**IPhone**手机等一切指纹密码保护都将被破解。

以下是 Imgur 的存档版本：imgur.com/a/uy7PY。

这场大抓捕行动中还有很多其他人被捕，以下是不完整名单：

Nicholas Powell and Michael Gonzalez

- *“TheSource,” “BonnienClyde,” BnC,” “BCPHARMA,” and “Money TS.*

Daniel Boyd McMonegal

- *“Sawgrass,” “Ross4Less,” and “ChristmasTree”*

Antonio Tirado and Jeffrey Morales

- *“TrapGod”*

Jeremy Achey

（EtiKing & Brohemoth）

Achey 案放在最后，它是一个很独特的案例。但本文不得不放弃其中一些细节，以便适应其他案例的水平。

这个伯利恒人（巴勒斯坦南部城市）不仅经营着相当多产的暗网供应商账户“EtiKing”，他还—以各种假名—积极参与“合法”的化学研究。

虽然有无数种匿名方面的操作错误导致 Achey 被捕，但其中一些错误肯定比其他错误更加突出。

[image]

根据刑事诉讼，2017年2月在佛罗里达州发生的致命药物过量引发了对 Achey 的调查。

验尸官的报告是这样写的：

> 结论：24岁的白人女性[受害者]的死亡是由于四氢呋喃芬太尼和依替唑仑的联合毒性导致的。死亡方式被归类为事故。

地方当局通知了缉毒局。 DEA分析了四氢呋喃芬太尼和依替唑仑，并确认了验尸官的报告。（此案发生时四氢呋喃芬太尼在美国还不是受控物质）

3月，DEA特工 Mark Bruso 和其他人联系了死者的家属，并了解到这对夫妇经常从 Alphabay 的一家名为 EtiKing 的暗网供应商那里购买产品。

特工检索了死者使用的账户，发现了死者曾经与 EtiKing 的通信信息，并确认了交易历史记录。

第一条信息就足以结束 **Achey** 的职业生涯了。这对夫妇在佛罗里达州收到的四氢呋喃芬太尼和依替唑仑包裹的包装上手写有以下寄回地址：USDTO # 6088 1321 Upland Drive，Houston TX 77043。

联邦特工重复使用钓鱼方法假扮买主，并证实了来自 EtiKing 的大部分包裹都有相同的退货地址。

[image] *U.S. Drug Testing Organization*

USDTO代表美国药物检测组织。

Achey 使用用户名 jeremysdemo，垃圾邮件链接到/ r / researchmarkets 和 / r / RCsources subreddits 上的网站。

使用用户名 jeremysdemo 和至少一个另外的类似用户名，Achey 主持了多个研究化学品的评价版。他甚至张贴了化学品研究网站用作他的 EtiKing 操作的一部分。

[image] *jeremysdemo*，*Jeremy Achey* 拥有的一个帐户，向*USDTO*发送垃圾邮件

EtiKing 的包装上的标记是支持比特币支付运费的公司 **Stampnik**。**Stampnik** 需要支付运费的人提供有效的电子邮件地址。

无疑 Stampnik 公司收到了传票，要求提供有关USDTO地址的所有信息，该公司提供的信息显示，EtiKing 已使用过至少九个电子邮件地址为其客户支付运费。

许多电子邮件地址可以将 EtiKing（和之前的 Achey）与研究化学领域的其他犯罪企业联系起来：

- brohemath@protonmail.com;
- getups@mail.com;
- getups@protonmail.com;
- onutra@protonmail.com;

- pbchems@protonmail.com;
- pbchems@ruggedinbox.com;
- stevemastermind76@yahoo.com;
- supernOva@protonmail.com;
- usdto@riseup.net.

[image]

政府间谍联系了一个秘密消息来源，该消息来源被描述为研究化学品、暗网市场和 Alphabay 的“精通”人士。

起诉书上写着，该机密消息来源最初创建并运营了 **EtiKing** 供应商账户。然后该消息来源以**400**美元的价格将该账户卖给了某人。该消息来源为当局提供了与**$400**交易相关的多个比特币地址。

[image]

几乎在所有暗网调查中当局的特工都会做同样的事 —— 他们转向求助于 Coinbase。有相关的比特币地址、物理地址和六个电子邮件地址，当局传唤了 Coinbase。

2017年6月，Coinbase 根据传票确认帐户所有者为 Jeremy Achey。

[image] Coinbase 的执法请求页面

Coinbase.com 为政府间谍提供了关于 Jeremy Achey 的以下证据：

- Achey 将其公司列为 “USDTO”，其网站为 USDTO.org，作为“慈善机构”和“独资企业”。
- Coinbase.com 记录显示，Achey 将

“brohemath@ruggedinbox.com” 和
“brohemath@protonmail.com” 列为其个人电子邮件地址。
Brohemath@protonmail.com 是 EtiKing 用于从 Stampnik 支付运费所使用的电子邮件地址之一。

- Coinbase 还对与调查相关的四个不同账户的数据进行了分析。

目前 Achey 被监禁在佛罗里达州萨姆特维尔的 USP Coleman I。无期徒刑。

结尾

以上这些错误都很常见。人们经常会同时使用多个网站、论坛上的账户，其中任何一个账户的错误操作都将是致命的。

[image]

返回：[image]S04完美隐身-总章节：机智是重要实力

我们对毒贩没有兴趣；本文想要说的是，当局能用这些方法抓住毒贩，他们就能抓住任何他们不喜欢的任何人 —— 包括仅仅是政治异议和所有说出真相的人。

我们希望您永远不要做坏事。但什么是好什么是坏，往往由当权者决定。如果你不幸被当局瞄准了，请尽可能不要犯低端错误 —— 哪怕你能让追踪者晕头转向足够长的时间，也很有可能成功消耗他们的金钱和精力；如果你幸运，追踪者会因此被耗尽，从而放弃你。

前车之鉴比安全知识更刺激，但前车之鉴必须落在对安全知识的强调上。

反追踪是一种心智的斗争。所以，请保持冷静，以便能令您的智慧充分发挥。

[image]
[image]

如何知道有人正在线人肉你？6个简单的方法

[image] 关键词	人肉 反追踪 数字足迹 自检 追踪
[image] 关联	[image]给活动家的反人肉指南
[image] 创建时间	2020年3月24日
[image] **Description**	操作安全性

追踪和反追踪用的是同一套方法，这或许就是这个互联网最有趣的地方 —— 正义和邪恶，谁掌握的技能多，谁就能获胜。

- Table of Contents

1、LinkedIn个人资料视图
2、为您的名字创建 Google 提醒
3、Facebook Story Viewers
4、Facebook 好友算法
5、Twitter Viewers
6、使用 Google Analytics（分析）创建个人资料网站
谁在找你？

[image]

如果您曾经尝试做过，就会知道，在几乎任何地方都有可能挖到关于您的真实身份信息 —— 其中也许包含很致命的信息，如果落在恶意者手里，将对您非常不利。

那么，您如何才能得知有人正在网上人肉你呢？幸运的是，其中大多

数资源都具有监视服务，您可以在有人搜索您的名字和相关重要信息时使用该服务来获取警报。

本文将介绍一些非常简单的操作，您可以设置警报或监视其他人何时使用互联网查询您的名字。

一共6个部分。

从最简单的开始。

1、LinkedIn个人资料视图

任何人都可以从 LinkedIn 内搜索您的名字，并以这种方式访问您的公开个人资料信息。

我们介绍过 **LinkedIn** 追踪的方法，在下面回顾：

LinkedIn 为会员提供了一种轻松的方法，以了解谁查看了您的个人资料。

要查看此信息，请登录您的 LinkedIn 帐户。在屏幕左侧的个人资料名称下，您会看到一个名为谁查看过您的个人资料的链接 。

在链接的右侧，您可以查看最近有多少人查看了您的个人资料。要查看更多详细信息，请单击链接。

向下滚动到 “All profile viewers” 部分。在这里，您将看到有关谁最近查看了您的 LinkedIn 帐户的一些详细信息。

这些信息包括：

- 名字

- 受雇的的公司

- 他们如何找到你的个人资料

- 您的 LinkedIn 人际关系中的哪些也与此人有关

- 他们在多久前查看了您的个人资料

不幸的是，您看不到查看过您个人资料的人的整个列表，除非购买高级LinkedIn会员。

如果您确实需要知道谁在查看您的 LinkedIn 个人资料，那么该高级会员身份可能是值得的。

调查人员任何避免这点？—— 当然是使用袜子木偶账户进行调查，即便目标人发现了你，他也不知道你是谁。 BACK [image]袜子木偶 - 分身创建的小技巧

2、为您的名字创建 Google 提醒

人们用来在互联网上查找有关您的信息的最常用工具是Google。

[image]

延伸：https://iyouport.substack.com/p/googledorking-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/d91?utm_source=publication-search

虽然您可能无法监视是谁在使用Google搜索你的名字，但是你可以监视何时有人开始挖你。

您需要一个提醒，以便在任何提及您名字的内容被创建时及时提醒你，请访问 Google Alerts。

[image]

确保您已经登录了Google帐户。在 “**Create an alert about**” 字段中，键入您的名字或者最常用的昵称再或者最关键的信息 —— 你知道自己最在乎什么，然后选择 “创建提醒”。

[image]

每当您将任何内容添加到Google提醒列表时，或者任何时候对包含您的姓名的网站进行新的搜索时，您都会收到一封有关该提醒的电子邮件。该电子邮件将包含指向提及您名字的网站的链接。

[image]

您会注意到，在电子邮件的底部，您可以单击链接以RSS提要的方式接收提醒。这将使您可以将提要添加到您可以使用的任何种类的提要阅读器中。

作为调查人员，如何避免被调查目标发觉？—— 很简单，不要用谷歌，使用更加私密的搜索引擎。

3、Facebook Story Viewers

Facebook 用户最常见的要求之一是想要知道谁查看了他们的 Facebook 个人资料。不幸的是，没有办法直接做到这一点。

但是，在 Facebook 的某些区域中，您可以看到访客。

如果您定期发布 Facebook 帖子，那么知道谁查看过您帖子的唯一方法是有多少“点赞”该帖子的人。可惜这不是准确的。

但是，当您添加到 Facebook Stories 时就不是这样了。如果您选择该字段来输入 Facebook 帖子，您会注意到可以将帖子从 “**News Feed**”

切换到 “**Your Story**”。

[image]

您可以将最多20秒的视频（或图像）发布到您的 Facebook Story 中。该信息将保持活动状态24小时，然后消失。

发布后您会注意到一个眼睛图标显示在该帖子的左下角，旁边有一个数字。

该数字代表的是查看过该帖子的 “朋友” 的数量。如果单击那个眼睛图标，则可以看到查看过该帖子的人都是谁。

[image]

如果您查看 Facebook 新闻源，那么在右侧可以看到指向您的故事的链接。

在左侧，您会看到带有 + 符号的个人资料照片。如果单击此按钮，可以查看所有最近的故事帖子，以及哪些朋友已查看这些帖子。

不幸的是，Facebook 没有为常规帖子提供此功能，但是至少在您发布到 “Story” 列表时，您可以看到所有查看过该帖子的朋友。那么很简单，您认为重要的内容就这样发布吧。

4、Facebook 好友算法

虽然看不到查看过您的特定 Facebook 帖子的朋友列表，但是可以通过间接的方式查看哪些朋友与您的 Facebook 个人资料互动最多。

如果发现可疑的莫名其妙的账户，拉黑TA。

[image]

没有人真的知道 Facebook 在好友列表中显示好友的顺序的具体细节。但是进行足够的研究后会能知道，它至少考虑了以下所有这些因

素：

- **Facebook** 互动：您与这些朋友在 Facebook 上互动的频率。
- 个人资料查看：这些朋友查看您的个人资料的频率、或您查看他们的个人资料的频率。
- 照片标记：在照片中添加了您的标签的朋友。
- **Wall Posts**：在你的时间线上发布的朋友。
- 点赞：他人点赞您的信息的频率，或者您点赞他们的信息的频率。
- 评论：您或朋友对彼此的帖子或图片发表评论的频率。
- 照片：你们查看彼此照片的频率。
- 在线：如果朋友当前在线，则更有可能出现在您的朋友列表的顶部。

由于 Facebook 上最常见的活动是查看目标人的个人资料和帖子，而无需与他们进行互动，所以，您能看到的朋友列表顶部的显示的人是最常查看您的个人资料和帖子的人。

5、Twitter Viewers

与 Facebook 相比，Twitter提供了更多有关关注者的信息，但仍未提供正在搜索您的人的姓名。

但是，您可以了解到有关与您的推文进行交互的人的很多信息。

要查看您的受众信息，您需要使用 Twitter Analytics。您可以通过单击个人资料名字旁边的向下箭头并选择 Analytics（分析）来访问它。

[image]

此页面将向您显示您的主要关注者是谁，以及所有推文的总体效果。

[image]

您可以单击查看关注者仪表板，以查看有关您的 Twitter 受众的常规详细信息。

[image]

您可以看到一些统计信息，例如性别、家庭收入和关注者的兴趣；这可能不会告诉您在 Twitter 上寻找您的人究竟是谁，但至少可以告诉您他们的兴趣倾向，以便您可以为关注者量身定制发布的主题。

对于调查人员来说，袜子木偶依旧是好的选择 —— 尤其是当您的调查对象是政府高官、僵尸牧民、信息战领军者等等，他们可能有很好的反侦察防备，所以您必修保护好自己的匿名性。

6、使用 **Google Analytics**（分析）创建个人资料网站

很多平台可以让你轻松建立自己的个人资料网站，其中包含有关您的背景和经验的信息。

个人资料网站是一种与潜在的雇主轻松分享您的背景和职业经历的绝佳方式。

如果您已经为自己的名字购买了一个网站域名，那么当人们搜索您的名字时，它也将成为最热门的搜索结果。

这将成为大多数人在网上寻找您时可能会点击的链接。

如果您将 Google Analytics 嵌入到此网站中，则可以收集有关在网络上查找有关您的信息的人员的大量信息。

Google Analytics 可能不会提供访问您网站的人的姓名，但是可以了解其他任何信息。例如：

- 年龄
- 性别
- 国家/地区
- 兴趣
- 访问频率
- 使用的搜索字词

这些信息可以使您深入了解在线搜索您的人的类型。

如果您是作家或从事向人们提供信息的任何其他公司或公民社会组织，那么这些信息可以帮助您和组织调整您的发布，以便令受众群更满意。简单说就是营销思路。

IYP不使用营销思路，我们提供的内容都是根据我们的民主经验认为成为一个合格公民所需要掌握的技能、知识、和技巧。

谁在找你？

如您所见，LinkedIn 和其他社交媒体网站是查看特定在线搜索对象的

最佳方式。但是 Google 提醒和您的网站也可以提供更多见解。

您采用哪种方法取决于您想了解目标什么样的信息。当然，最有效的永远是开源情报调查 —— 并不是所有人肉贩子都擅长完美的袜子木偶；糟糕的袜子比比皆是，挖出其背后的真实身份可能不难。

简单说就是反向追踪：Watching The Watchers。易于追踪是这个互联网的本性，追踪技术被谁掌握，将决定它是正义还是邪恶。

[image]
[image]

如何检查您的VPN连接是否实际加密

[image] 关键词	VPN 反追踪 自检
[image] 关联	[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话
[image] 创建时间	2020年4月24日
[image] **Description**	操作安全性

这是合理的偏执，肯定比后悔更好。

- Table of Contents
在Mac上验证加密
在PC上验证加密

[image]

先关联一个去年底的消息。

[image]

不要使用“TurboVPN”。该vpn声称不保留日志，但这不是事实。其隐私政策中你可以看到（下图），它收集各种用户信息，这与真正的无日志服务完全相反 —— 这个隐私政策非常难以找到，如果你使用电脑基本是找不到的。

[image]

Turbo 只有在使用“最快服务器”时的表现才稳定。而一旦连接中断，你的流量很容易因此暴露；同样，所有没有自定义DNS设置的VPN都

无法100%保证你的安全。

Turbo VPN 无法在中国下载，这可能是个障眼法。您需要小心：并不是所有被 App Store 下架的VPN都是“安全的”。

很多VPN声称自己是加密的，那么你怎样才能得知它们是不是骗子呢？

其实不需要您学会怎么玩数据包嗅探器和协议分析器，一个网络实用程序就可以做到，它使您可以查看从您的计算机来回传输的数据。

在未连接到VPN时检查一次，并捕获了一些数据包，然后在连接后再做同样的事。很简单就可以看到传输的数据在发送到VPN时是否已经加密。

无需技术专长。您所需要做的就是按下一个记录按钮，滚动列表并检查一些文本。

您可以忽略其他所有内容，因为除非您对计算机和网络有所了解，否则您不需要那些东西。

在Mac上，使用 CocoaPacketAnalyzer，在PC上，使用 Wireshark。

在Mac上验证加密

首先，在Mac上下载 CocoaPacketAnalyzer 并运行它。您应该看到带有四个大按钮的启动屏幕。

[image]

点击 Capturing 即可开始捕获网络流量。如果您保存捕获会话，则称为 trace file，稍后您可以使用第二个按钮再次打开它们。

出于本文的目的，我们只希望看到数据是否已加密，因此不需要也不会保存任何捕获数据。

在执行捕获之前，请继续并单击“首选项”以设置如何捕获数据。

单击顶部的 **Capture**，需要在此处检查的唯一设置是 **Capture Interface**。

[image]

首先请确保按下列表框右侧的刷新小按钮。

当您点击该框时，您会看到几个选项，所有这些看起来都很混乱。不要管它，您唯一需要选择的就是列出了 **IPv4** 并带有一些数字的那串东西。

您无需选择包含127.0.0.1的那个，需要选择一个具有当前正在使用的连接的IP地址的条目。您可以通过转到“系统偏好设置”，然后单击“网络”来解决此问题。

[image]

单击左侧列表框中带有绿点的连接，然后检查右侧部分的IP地址字段。

如您所见，它显示为 192.168.1.x，因此与程序下拉列表中的 **en0—IP4–192.168.1.68** 选项匹配。

现在关闭 “Capture Preferences” 窗口，以返回到主屏幕。

继续并单击 “**Capturing**”，现在将弹出一个新对话框，您可以在其中选择一些设置，然后开始捕获。

[image]

在这里您不需要进行任何更改，因此要开始使用，只需按 **Start**。

但是，在执行操作之前，需要注意一些事项。

首先，您应该尝试关闭所有正在运行的程序和任务栏程序，并仅使浏览器窗口保持打开状态。这是为了尽可能减少数据流让任务变得简单一点。

之后，立即加载一个或两个站点，然后单击“停止”。您只需要捕获几秒钟就够了。您甚至可以直接在浏览器的标签页中输入网址，那么一旦开始捕获，您只需按Enter即可加载页面。

按下 “Stop” 后，您将看到一个类似于下面的窗口：

[image]

现在它看起来像是胡言乱语，这就对了。您需要做的就是滚动浏览顶部的列表（表格格式），然后查看在右下角的框中看到的数据，在上面突出显示了该数据。

由于可能有成千上万的行，您只需快速按下向下箭头并查看底部的数据更改即可。

[image]

如果您的VPN连接实际上是加密的，那么滚动的每一行都应显示与上图中的数据相似的样子。

由于它不可读，只有一堆随机字符，因此可以判断已加密。

使用加密的连接，那数千行中的任何一行都不应该被读取任何内容。

现在要不要看一下在未加密的连接上（例如未连接到VPN时）看到的内容？就是下面这样：

[image]

如上所示，由于没有加密，因此可以阅读到很多的内容。你能看到主人使用了 Mac 和 Safari，访问了aseemkishore.com，以及许多其他数据……

并非每个数据包在未加密的连接上都是可读取的，但是对于大多数数据包来说，您都能够看到实际数据，HTML代码、协议标头等。

在PC上验证加密

在PC上进行检查的过程与上面显示的过程几乎相同，除了您使用的是名为 Wireshark 的程序。

下载后，将其启动，主屏幕应如下所示：

[image]

就像在Mac上一样，您需要做的第一件事就是选择要为其捕获数据的接口（网络接口）。点击“接口列表”，您将看到网络接口列表。

我更喜欢 Wireshark，因为您实际上可以看到每个接口上正在传输多少数据，这使您很容易看出哪个是主要连接。

[image]

继续并选中相应接口旁边的框，然后单击“关闭”。

现在，您所要做的就是单击“开始”按钮（在“接口列表”按钮下方），您将可以正常使用；您无需更改任何其他选项。完成捕获后您应该会看到如下屏幕：

[image]

您可能必须全屏展开，然后相应地调整底部和顶部窗格，但是您可以看到数据的格式与Mac上的 CocoaPacketAnalyzer 完全相同。

滚动浏览顶部的列表，并确保数据部分完全是乱码，这意味着您的连接已加密。

如果您能够阅读任何单词或文字，则表示数据未加密。确保使用箭头键快速浏览至少几百行。

希望您的VPN连接被证实已经安全加密。

[image]
[image]

攻击者如何收集有关目标的情报？他们能了解你多少？

[image] 关键词	对抗性思考方式 开源情报 自检
[image] 关联	🔍开源情报
[image] 创建时间	2020年5月21日
[image] Description	操作安全性

这里是关于开源情报的精减版，您能从中掌握对该领域的整体了解。

- Table of Contents

  什么是开源情报？
  开源情报干什么用？
  开源情报框架是什么？
  其他开源情报工具、技术和资源
  最后

[image]

进行任何有针对性的攻击（或进行渗透测试、或红队活动）的第一步是收集关于目标的尽可能详尽的情报。

尽管有多种方法可以秘密进行收集，但情报收集通常都会始于从公共资源中抓取信息，这些信息统称为开源情报。

由于社交媒体和在线活动的盛行，现在有大量合法可收集的开源情报可用，这些信息很可能为攻击者提供成功描述组织或个人所需的一切。

政府间谍经常这么做，他们称之为“社交媒体情报”，该领域甚至不在法律可约束范围内，见 BACK https://iyouport.substack.com/p/842?utm_source=publication-search。

什么是开源情报？

开源情报是指可以合法地从有关个人或组织的免费公共来源中收集的任何信息。

开源情报不是新鲜事物，它已经有一百年的历史 —— 2018年是它的百年纪念。

实际上，这往往意味着可以在互联网上找到的所有信息都属于开源情报。

从技术上讲，任何公共信息都属于开源情报类别，无论是在公共图书馆中的书籍或报告、报纸上的文章还是新闻稿中的声明。

开源情报还包括可以在不同类型的媒体中找到的信息。尽管人们通常认为它是基于文本的，但是图像、视频、网络研讨会、公开演讲和会议中的信息都属于开源情报。

简单说，只要你能挖出来（而不是偷），它就属于你。

开源情报干什么用？

通过收集有关特定目标的公开信息源，攻击者（或友好的渗透测试人员）可以精准地描述潜在的受害者，以便更好地了解其特征、并缩小搜索范围，以寻找可能的漏洞。

以此来制定可能最有效的攻击计划。

攻击者无需主动与目标交战，就可以利用产生的情报来构建威胁模型和制定攻击计划。

像军事攻击一样，有针对性的网络攻击同样始于侦察，而数字侦察的第一阶段是被动地获取情报而不会警告目标。

将开源情报收集运用到您自己或您的组织上，是了解您为潜在的攻击者提供了哪些信息的好方法。

一旦您知道可以从公开来源收集到什么样的情报，就可以使用它来帮助您自己或您的团队制定更好的防御策略。

您的公共信息暴露了哪些漏洞？攻击者可以从中了解到什么，他们可以利用其进行哪些社交工程攻击或网络钓鱼攻击？

帮自己回答这些问题。

开源情报框架是什么？

从各种各样的来源收集信息是一项耗时的工作，但是有许多工具可以简化情报收集。

虽然您可能听说过 Shodan 之类的工具、以及 Nmap 和 Zenmap 之类的端口扫描仪，但相关工具种类繁多。 BACK https://iyouport.substack.com/p/15f?utm_source=publication-search

安全研究人员本身一直在记录可用的工具。

贾斯汀·诺丁编写的开源情报框架是一个很好的起点。该框架提供了指

向大量资源的链接，这些资源用于执行各种各样的任务，从收集电子邮件地址到搜索社交媒体或暗网。

[image]

在许多有关开源情报工具的文章中，您都会看到对 Kali Linux 渗透测试发行版中包含的一个或两个软件包的引用，例如 The Harvester 或 Maltego；要了解可用于 Kali 的开源情报工具的完整概述，请查看 Kali Tools 列表。其中提供了这些工具的简要介绍以及如何使用每个工具的示例。

[image]

在这里，您可以找到许多有用的开源情报收集工具，其中包括 Nmap 和 Recon-ng 等研究人员最喜欢的工具。

Nmap 工具允许您指定IP地址，例如，确定哪些主机可用，这些主机提供哪些服务，它们运行的操作系统，正在使用的防火墙、以及许多其他详细信息。

[image]

Recon-Ng 是 Tim Tomes 用Python编写的用于网络侦察的工具。您可以使用它来进行枚举给定域的子域之类的事；一旦添加了适当的API密钥，就有许多模块可以让您涉足 Shodan、Github、Jigsaw、Virustotal 等。

模块按类别进行分类，例如侦察、报告和发现。

[image]

其他开源情报工具、技术和资源

当然，用于情报收集的最明显的工具之一是Web搜索引擎，例如 Google、Bing 等等。

实际上，有数十种搜索引擎，对于特定类型的查询，某些搜索引擎可

能会比其他搜索引擎返回更好的结果 —— 请查看上面的汇总链接。

问题是，如何有效地利用所有这些引擎呢？

Searx 是一个很好的工具，可以解决此问题并使Web查询更有效。

Searx 是元搜索引擎，可让您匿名同时收集来自**70**多个搜索服务的结果。

Searx 是免费的，您甚至可以托管自己的实例以获取最终的隐私。既不跟踪也不对用户进行概要分析，并且默认情况下禁用 cookie。 **Searx** 也可以在**Tor**上用于在线匿名搜索。

[image]

Searx 的许多公共实例也可供那些不想或不需要托管自己的实例的人使用。有关列表请参见 https://searx.space/

[image]

一直有很多人在为开源情报社区开发新工具，跟踪新信息的最好方法就是推特。但是，在 Twitter 上跟踪事件可能有点困难。幸运的是，还有一个开源情报工具叫做 **Twint**。

Twint 是用Python编写的 Twitter 抓取工具，可轻松匿名收集和寻找 Twitter 上的信息，而无需注册 Twitter 服务本身、也不必使用API密钥，就像使用 Recon-ng 这样的工具一样。

使用 Twint，完全不需要身份验证或API。只需安装该工具并开始搜寻即可。您可以按用户、地理位置和时间范围等进行搜索。这只是 Twint 的一些选项，也有许多其他选项可用。

[image]

那么，如何使用 Twint 帮助您跟上开源情报的发展呢？好吧，这很容易，并且是 Twint 在行动中的一个很好的例子。

由于 Twint 允许您指定 -since，以便仅从特定日期开始提取推文，因此您可以将其与 Twint 的搜索词结合使用，比如每天抓取标有#OSINT的新推文。

您可以使用保存为 SQLite 格式的 Twint 的 -database选项，自动执行该脚本并将结果输入数据库中，以方便您查看。

测试一下。到目前为止，看起来好像有58条#OSINT推文。

```
twint -s '#osint'—since 2019-07-17
```

[image]

可以用来收集公共信息的另一个很棒的工具是 Metagoofil。该工具使用 Google 搜索引擎从给定域中检索PDF、Word文档、Powerpoint 和Excel文件。

然后，它可以从这些文档中自动提取元数据，以生成一份报告，列出诸如用户名、软件版本、服务器和机器名之类的信息。

[image]

最后

本文介绍了开源情报的基本概念以及它为何有用。

并且在几个不错的地方找到了很多开源情报工具，这些工具可以帮助您收集所需要的几乎所有类型的信息，并且还向您介绍了一些单独的工具，展示了它们如何可以投入工作。

对于任何参与网络安全的人来说，了解如何收集开源情报都是一项至关重要的技能。

[image]

不论您是想保护自己、还是保护自己的组织和团队，您对数字足迹的了解越多 —— 越擅长从攻击者的角度审视防御，您的防御能力就越强。

有了这些知识，您就可以继续制定更好的防御策略。

[image]
[image]

如何识别手机上的恶意软件？

[image] 关键词	恶意软件 移动设备 自检 防御
[image] 关联	[image]当您准备像编程随想那样工作...：须知 ；[image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 ；[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人 ；[image]设备好像被黑了怎么办？ - 数字急救包
[image] 创建时间	2020年7月29日
[image] Description	操作安全性

人类如果感染病毒会发烧咳嗽，手机感染病毒的结果也会出现一些“症状”，让您知道它病了。这些症状也许不够明显，您需要在多个方面保持警惕以及早移除病灶，至少是本文中列出的这些方面。

- Table of Contents
如何确定我的手机是否感染了病毒？
1、数据使用量突然增加
2、耗电量增加，明显比平时更费电
3、智能手机的性能突然下降
4、智能手机开始过热
5、陌生的应用程序开始显示在设备上
6、Wi-Fi和移动数据自动开启
7、弹窗广告
结论

[image]

恶意软件和间谍软件是最常见的两个计算机安全问题。虽然确实很容易使计算机感染恶意软件，但重要的是不要忽视移动设备也很受到影响这一事实。

当智能手机感染了恶意软件时，它可能会导致多个问题，包括被监视、被跟踪、被骇客从受害者那里窃取最私密的信息，等等。

对于任何智能手机用户来说，了解如何检查自己的手机是否感染了病毒，是重要的一步。

有几种迹象可能表明设备上存在病毒，如果您识别出了这些迹象，立刻采取适当的措施至关重要，例如 使用可靠的防病毒软件。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

如何确定我的手机是否感染了病毒？

智能手机用户必须意识到随时可能出现的诸多威胁，包括攻击者现在执行的最新DNS劫持。

感染后的手机难以检查病毒会导致多种问题，包括 勒索软件、密码盗取、窃取机密数据等等。此外，还有一些恶意软件也可能导致智能手机的物理功能出现问题。

以下7个迹象表明您的智能手机已被恶意软件感染：

1、数据使用量突然增加

在查看手机是否感染病毒时，最早出现的迹象之一就是数据使用量会突然增加。

即使智能手机上的某些应用程序和游戏可能会占用大量数据，但在没有明显原因的情况下使用的数据量突然增加时，这可能表明手机已感染病毒；尤其是 ADB.miner 之类的恶意软件以在 Android 手机和智能电视上挖掘 Monero 币而闻名。

iOS 和 Android 都在 “设置” 部分提供了一个功能，使智能手机用户可以大致了解自己的设备上正在使用多少数据。

Android 设备也将能够提供一个图表，显示指定时间段内的数据使用情况 —— 这样就很容易检测到突然增加的情况。

对于 Android：

- 打开手机的“设置”应用。
- 点击 Network & internet ＞ Data usage.
- 在 “Mobile” 下，您会看到您使用了多少数据。
- 要查看图表和详细信息，请点击 Mobile data usage；要选择时间，请点击向下箭头；要查看每个应用使用了多少数据，拉到图表下方。

对于 iPhone：

要打开或关闭蜂窝数据，请转到 “设置”，然后点击 “蜂窝数据” 或 “移动数据”。如果您使用的是iPad，则可能会看到 Settings ＞ Cellular Data；如果您使用的是双SIM卡 iPhone，则需要将其中一个号码设置为主要数据。

2、耗电量增加，明显比平时更费电

这是另一个感染迹象。尽管有时这可能表明电池已损坏，但仍有多种病毒可能会导致智能手机电池快速耗尽。

所以依旧要建议您在花钱更换电池之前，应该首先对手机进行排除感染的扫描。2019年2月，研究人员揭露了一项名为 DrainerBot 的 Android 主要广告欺诈骗局，其特征就是费电和吞噬设备数据。

3、智能手机的性能突然下降

市场上一些较新的智能手机倾向于配备功能强大的处理器和足够的 RAM，以轻松处理应用程序和游戏中使用的最新技术。

当装有这种技术的智能手机突然开始出现性能降低的情况时，也可能表明该设备已感染病毒。

这也许不大容易被注意到。有时只有进入需要强大CPU和GPU的游戏时，性能下降才会引起注意。

而在其他情况下，病毒也可能导致移动设备的整体性能下降，即使执行简单的任务（如拨打电话或阅读短信）也是如此。

4、智能手机开始过热

除了发现智能手机的性能不足外，过热可能是另一个迹象表明它已被 HiddenMiner 之类的恶意软件感染。

在大多数智能手机中这都是一个罕见的问题。因此，当出现过热问题时，病毒扫描可以帮助检查手机上的恶意软件。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

5、陌生的应用程序开始显示在设备上

感染智能手机的病毒有时可能会导致您不熟悉的应用程序被自动安装。

因此，如果有一些应用程序在用户不知情的情况下出现在手机上，就可能是该设备已感染病毒的又一个迹象。

当该应用程序看起来很可疑时，不仅应将其删除，而且，还应彻底扫描设备本身以查找可能的病毒的残留痕迹。

6、Wi-Fi和移动数据自动开启

您应该时刻警惕移动数据和Wi-Fi开关。由于病毒通常会通过互联网发送和接收数据，在用户禁用移动数据或Wi-Fi连接后感染也可能会导致数据被打开。

7、弹窗广告

另一个烦人但很明显的迹象是弹出广告的突然出现。即使在用户离开应用程序并留在手机首页后，这些内容仍然会显示出来。

这类弹出广告有时会显示不适当的内容，或将用户引导至智能手机应用程序商店中。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

结论

恶意软件会同时影响台式计算机和移动设备。当智能手机受到影响时，问题可能更严重，因为那上面通常都有银行卡和信用卡的详细信息。

如果您怀疑自己可能受到感染，就需要了解如何确定病毒的存在；这可以帮助您采取措施删除病毒以保护您的敏感数据。

[image]

返回：[image]设备好像被黑了怎么办？ - 数字急救包

[image]
[image]

在线组织和互助需要多方面小心以维护所有参与者的安全：基本注意事项

[image] 关键词	互助 加密 反监视 团队 威胁模型 战略策划 数据安全 监视资本主义 组织 自卫
[image] 关联	[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09 ；[image]直接行动分步指南：它是什么、它有什么用、如何获得成功
[image] 创建时间	2020年8月18日
[image] **Description**	操作安全性；行动安全性

在线组织民间互助组是疫情中直接行动的最佳实践。但组织者和联盟协调人员需要注意一些安全问题。

- Table of Contents

  以下是组织者需要牢记的安全注意事项：
  为什么在组织互助时数据安全很重要
  网络钓鱼：
  人肉弱势群体并促进针对性的骚扰：
  政府收集：
  数据销售：
  确定您的目标受众（和非目标受众）
  收集尽可能少的数据
  注意权限，对访问透明
  加密一切
  考虑信任和社区数据的敏感性

其他要考虑的事
收集和共享信息
1、定义您的受众
2、收集尽可能少的数据
3、注意权限，尽可能限制访问
4、使用加密
5、此外
6、对于参与者来说，请检查组织者是否明确传达了以下信息：
了解您的风险：

[image]

各种各样的社区都在加紧组织互助团体，以虚拟方式团结起来，为需要帮助的人提供和协调支持。

为了满足防疫需求上的身体距离，许多人正在使用Google电子表格、Twitter 和 Facebook 上的公开帖子、以及社交媒体平台上的私人消息进行在线组织。

这种支持具有强大的能力，但同时也引起了安全方面的关注：被忽视的隐私设置和过分的个人数据收集会导致意外地泄露私人信息，这些信息的泄漏不仅对活动家本身是危险的，而且很容易损害任何寻求帮助的人们。

尽管这些努力似乎在帮助有需要的人与资源之间建立联系方面具有同等的好处，但是，其使用的媒介本身的隐私和安全隐患却完全不同。

EFF为组织者和志愿者提供了数字安全和隐私注意事项的指南，以更好地保护他们所支持的社区。

以下是组织者需要牢记的安全注意事项：

1、定义您的受众群体 —— 您想吸引谁，如何吸引他们，以及您想要为他们做什么？

2、收集尽可能少的数据 —— 实现目标实际所需要的数据是什么？以及对社区来说最敏感的数据是哪些？

3、注意权限，并在可能的情况下限制访问 —— 您的数据需要全部公开吗？您可以限制它仅被社区中的一小部分人可见吗？

4、在旅途中和休息时使用加密 —— 您正在使用哪些工具？谁可以看到您的数据？它受到保护吗？

5、考虑一下您信任哪些公司、人员和系统掌握您的敏感数据 —— 您可以通过端到端加密平台连接参与者吗？

这些都是组织者在设计这些工作时应该考虑的所有问题，参与者应该有能力向组织者询问这些问题。

组织过程中共享的信息可能非常敏感，并且是潜在的网络钓鱼尝试的主要目标。参与这些工作的每个人都必须了解风险是什么，以及如何通过深思熟虑的数据保护措施来将风险最小化，这一点很重要。

为什么在组织互助时数据安全很重要

本文将假设一个行动组织者名为 Layla，以分析其经历。 Layla 认识到，迫切需要努力将需要财务支持的人员与帮助者联系起来，并获得资源。

她决定建立一个带有易于查看的相应文档的网站，以便帮助人们共享和推广他们的需求，并提供一种进一步联系的方式。

但是，这样做时，Layla 决定要保护自己社区的敏感数据免受恶意攻击。

个人数据可能会以多种方式被滥用，不幸的是，有很多恶意者经常想要在不确定性和压力很大的时期利用他人的脆弱性。以下只是一点点示例：

网络钓鱼：

在了解有关目标情况的非常具体的信息时 —— 例如，他们的电子邮件、Venmo 或银行信息、他们的真实姓名、地址、他们寻求帮助的情况、他们的健康信息、以及他们的故事，恶意者就会欺骗目标。尤其是，恶意者会利用发现的尽可能多的信息来了解其目标，从而制作出听起来更真实的骗局。

Layla 需要思考如何限制这些信息的可见度，并确保仅在绝对必要时才收集参与者的敏感数据。

[image]

激进社区用户请从这里进入：[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

人肉弱势群体并促进针对性的骚扰：

恶意者可以发布有关某人的生计、工作场所、和家庭住所的私人信息，以骚扰他们。这是 doxing 的典型操作。

[image]

返回：🕷人肉搜索

返回：[image]给活动家的反人肉指南

返回：[image]如何知道有人正在线人肉你？6个简单的方法

这种骚扰可以是数字层面的、财务方面的和现实物理层面的。数字层面的骚扰通常采取网上辱骂的形式；财务骚扰可能意味着将这些信息用于欺诈性账单；在其他情况下，攻击者会不断发送垃圾邮件，直到用户意外接受为止。

现实物理层面的骚扰包括很多种形式，从尾随纠缠到恶作剧、殴打、报假警让警察集体围攻目标人的住所等等。

即使在正常情况下，这些活动也可能危及一个人的生计或安全。对于那些已经被边缘化的或特别受时事影响的人们，会更加有害。

由于 Layla 支持的是有可能将其私人信息被用于有针对性的骚扰的社区，因此她需要仔细考虑如何保护这些信息，以免被恶意者掌握。

政府收集：

全球政府都在大规模收集有关公民的私密详细信息。在最有害的情况下，政府机构之间的这种数据收集和共享可能使已经被定位的社区面临更大的风险，尤其是在可能已经对某人进行监视的情况下 —— 由于其移民身份、性别、性取向、健康状况、经济状况、信仰、种族、或政治联盟。

就 Layla 而言，她特别担心移民和海关执法局进一步针对她所在社区的人们，并且不希望收集那些可能被滥用以促进突袭的信息。

[image]

返回：https://iyouport.substack.com/p/lr--6f2?utm_source=publication-search

返回：👁👁大规模监视

数据销售：

不论是大型还是小型公司都在不断抓取网络数据以获取有关他们可以汇总和出售的个人的信息，例如第三方跟踪所做的。这就是监视资本主义。

Layla 的社区成员担心，共享信息可能意味着他们最终会出现在更多的垃圾短信和电话营销列表上，或者被多家公司跟踪。

这些都是棘手的问题，会带来可怕的后果。组织者应该考虑使用以下概述的原则，采取实质性的预防措施来防止这些不良后果。

考虑到所有这些潜在威胁，Layla 知道她想保护社区成员提交的数据，她意识到自己收集的数据非常敏感。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

使用 “威胁建模” 框架，需要思考以下问题：

1. 我想保护什么？

1. 我想防备谁？

1. 如果我失败了，后果有多严重？

1. 这些威胁发生的可能性有多大？

1. 我愿意为了防止潜在后果付出多大的努力？

以下是帮助 Layla 这类组织者回答上述问题时的注意事项。

确定您的目标受众（和非目标受众）

在思考有关构建社区安全计划的问题时，通过此工作来确定您的目标并确定倡议的规模，可能会有所帮助。考虑以下问题。

- **1**、我想联系谁？

这是针对邻里社区（由彼此认识的20个多位邻居组成的小组）、本地社区（乡镇或县内的人们，多达数百人）、还是更大的社区？不同模式的社区具有不同的安全计划。

- **2**、您可以清楚地与参与工作的人交流什么？

计划一开始就要建立期望 —— 不仅是寻求和提供帮助的人们，而且还要包括有希望扩大您的努力的外部团体。

当前参与您的组织的人与其他组织的工作也存在很大的交叉关联趋势，并且有可能使您原本打算更封闭的组织工作最终获得了比预期更多的知名度。

要清楚地说明对这个社区的要求：考虑如何使流程对刚加入该计划的人透明：当他们提交请求时，他们期望多少天内能得到答复？如果响应及时实现或没能实现，会发生什么？该文档及其中的数据将被如何处理？

您需要多少数据来组织该援助？不同的受众可能需要不同级别的数据收集。这就需要考虑下面一点。

收集尽可能少的数据

连接人们以实现互助肯定需要您共享有关参与者的一些信息。

但是重要的是，要注意某些类型的数据的敏感性，尤其是有关一个人的病史、地理位置和具体身份的信息。

收集尽可能少的数据来实现您的目标有助于降低不良行为者获取足够信息以伤害目标人的风险。

某些类型的可识别性信息对于社区共享而言，其风险可能要比其他类型的信息稍低一点。例如，Layla 可能知道她所在社区中的某些人担心公开自己的电话号码，因此选择仅在她的表格中包含一个电子邮件地址字段。

名字和电子邮件地址就可以帮助她识别参与者，因此她还决定不需要存储社区成员的姓氏。

她还可以鼓励社区成员使用不包含名字和姓氏的电子邮件地址。

于是，如果数据落入坏人手中，那么他们将很难识别每个参与者。

考虑需要将这些信息保留多长时间也非常重要。删除不再需要的信息是一种很好的安全措施。一些组织者使用电子表格之类文档来组织一次性工作，而无需永久保存数据。

由于您的社区可能有不同的需求和关注点，因此您应该回答以下一些问题，以确保您仅收集了严格必要的内容：

- 您需要什么类型的信息才能实现这一组织行动的目标？
- 您要求的数据中是否存在冗余？如果是，您可以删除其中一些字段吗？
- 哪种类型的数据对您的社区最敏感？您能否要求提供一条不同的、不太敏感的替代信息，并且仍然可以实现您的目标？

- 您什么时候可以删除此电子表格和提交的数据？

注意权限，对访问透明

在 Venmo、Facebook 帖子或 Google 表格等服务中，用户可以通过调整设置来限制可见性。

例如，使用 Venmo 的用户可能会惊讶于默认情况下其所有交易都是公开的。用户可以将其交易设置调整为 “私人”，仅对发送者和接收者可见；但是，Venmo 始终会公开显示您与谁进行了互动的记录。

同样，可以将 Google 产品（例如文档和表格）设为私有，以便仅在受信任社区内的受邀电子邮件地址中可见；通过限制某些朋友或社区的可见度，可以使 Facebook 帖子更加私密。

但是 —— 您必须按顺序阅读本文 —— 首先应该是您的威胁模型，如果您组织的是类似透明度革命协作社区，那么以上这些最好都不要使用，因为它们都来自寡头，这些寡头与政府紧密合作，可以在任何政府请求下出卖你们所有人。

并且，权限和访问注意事项超出了单个工具的范围，组织者需要从头开始考虑它们。

例如，Layla 可能会考虑使用 Google 表格来让其社区向志愿者提交援助和要约请求，而不是使用任何人都可以公开访问的可见的和可编辑的文档。

Layla 可能会稍为取舍，因为 Google表格需要一些受信任的人来审核请求，因此她可以选择与社区成员清楚地交流该过程。

或者，也许Layla决定只充当中间人，通过电子邮件介绍服务将寻求帮助的人联系起来，并鼓励他们使用端到端加密工具来传达更多详细信息。

加密一切

加密有多种类型，熟悉与在线组织动员工作有关的加密会很有帮助。

在选择一种促进交流的方法时，考虑一下谁可以看到哪些数据以及如何存储和保护这些数据，是很重要的。

通过互联网访问服务时，您的流量、及其所有提交的内容（“数据”）、有关内容的信息（“元数据”）），都将通过多个实体控制的多个设备，然后到达预期的目标设备。

[image]

要考虑的一件事是，数据如何在传输中移动：人们如何共享信息，如何沟通其需求和服务，如何相互联系？又如何使它尽可能安全？

通常，端到端加密是保护通信数据仅在发送方和接收方之间可获取的最佳选择，因为它在用户的 “终端” 设备之间进行加密。

但是，在加入端到端加密服务之前，人们首先需要了解这项行动/工作的具体内容，他们可能首先会通过网站来了解它。

于是就不得不提出下一个重点：警惕未加密的服务和网站。例如，如果服务仅使用HTTP（而非HTTPS）来收集从表单提交的信息，则意味着其敏感数据未加密。

如果您是诸如 Layla 这样的网站运营者，则可以通过 Let’s Encrypt 获得免费的 HTTPS 证书。

对于那些希望通过民间互助组获得帮助的人，请警惕不使用加密的服务。

考虑信任和社区数据的敏感性

好消息是，网络上的大多数服务都使用 HTTPS 保护传输中的数据。但是，仅仅如此并不一定意味着该服务值得您的信任。

这是您认识的那个人经营的网站吗？您是否信任他们来保护您提交的数据？还是像 Google，Facebook 或 Twitter 这样的寡头？服务提供者是否为文档和帖子提供了不同的设置选项，例如 “公开”、“私人”、或仅限于一小部分人？

特别是，请问自己以下问题：

- 您在此平台上收集的数据有多敏感？
- 您相信服务提供商的安全能力吗？
- 您相信他们会负责任地处理您社区的数据吗？
- 如果您不信任他们，该怎么做？

对于某些人的安全计划而言，知道像 Google 或 Facebook 这样的寡头公司可以看到其在平台内的所有通信是一个可以接受的风险 —— 但是，对于另一些人来说，尤其是那些试图挑战政府和间谍机构值权威的人们，这是非常危险的。

后者应该使用那些更具隐私保护的产品或使用端到端的加密服务。

[image]

对于 Layla 来说会鼓励她的社区使用 Signal 之类的工具来交流有关他们自己的更多详细信息，因为她确定自己不需要收集哪些私人信息。

[image]

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

其他要考虑的事

随着 Layla 的组织工作越来越受到关注，她可能会考虑与其他公民社会组织形成联盟，以扩大他们的工作。

但是，每个组织的工作都有不同的安全计划，并且在宣传方面或形成联盟关系时可能会需要考虑不同程度的问题。

对于创建这些汇总文档的人来说，一个很好的做法是，分别询问每个组织者是否可以接受某种做法。

此外，联盟负责人可能还希望考虑不同组织发布的信息类型之间的差异。范围从非常敏感到敏感性较低，需要准确评估。

对于那些汇总和汇编跨组织信息的联盟负责人来说，请考虑以下问题：

- 您为什么要汇总这些信息？您的目标是什么？
- 您要放大哪些不同类型的数据或信息？他们是否需要不同的隐私考虑？
- 您真正需要什么信息来使数据聚合对人们有用？
- 在链接到较小的数据源之前，您可以与具体的组织者事先交流一下吗？征求他们的意见关于他们想要公开哪些和隐藏哪些。

将安全计划制定流程纳入组织的工作是确保为您和您的社区保证安全标准一致的好办法。

收集和共享信息

1、定义您的受众

您想联系谁？您的受众对他们的需求有什么期望，他们如何获得信息更新以及数据的可见性如何？谁不应该访问此信息？

2、收集尽可能少的数据

您要实现目标所需要的最少量数据是哪些？哪种类型的数据对您的社区最敏感？您可以要求替代敏感数据的其他类型数据吗？

3、注意权限，尽可能限制访问

您需要公开所有数据供人们访问吗？如果不是，您可以将权限限制在社区的较小部分中吗？

4、使用加密

对于您正在使用的服务或平台，考虑谁可以看到哪些数据？您的数据在发送或存储的过程中是否受到保护？

5、此外

- 您能否会建议使用更安全的渠道来跟进更多详细信息？
- 您可以通过端到端加密平台联系所有参与者吗？端到端加密通信有助于保护通信数据在预期的发送方和预期的接收方之间。

对于那些为跨组织联盟工作努力的人们，请注意以下问题：

- 您为什么要汇总？您的目标是什么？

- 您要放大哪些不同类型的数据或信息？它们是否需要不同的隐私考虑？

- 您真正需要什么信息来使数据聚合对人们有用？

- 在链接到较小的数据源之前，您可以与具体的组织者事先交流一下吗？征求他们的意见关于他们想要公开哪些和隐藏哪些。

6、对于参与者来说，请检查组织者是否明确传达了以下信息：

- 您的参与期望是什么

- 提交哪些信息是必需的哪些是不必需的

- 参与平台是否使用加密，并确保至少使用HTTPS

- 数据的公开程度如何、以及组织者能看到多少数据

- 数据将存储在哪里以及存储多长时间

- 是否有端到端加密通信工具可以围绕敏感细节进一步与参与者建立联系，以及如何将这些细节与视野更广的平台区分开

了解您的风险：

- 您可以与组织者沟通这些问题并讨论他们为缓解这些问题而采取的步骤吗

- 注意与所提供信息有关的潜在网络钓鱼企图。

- 考虑一下您可以忽略的内容：是否需要提供真实姓名或其他可识别性信息，例如电话号码或家庭住址？如果您的电子邮件中包含您的真实姓名，您可以使用其他的与您的身份无关的电子邮件吗？

直接行动正是因为政府的迟钝和不作为公民需要自己动手维护自己的利益。于是公民组织必须做得比政府更好，给参与者更多的安全和权益。希望这篇文章中介绍的注意事项能对您的社区有所帮助。

[image]
[image]

您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

[image] 关键词	分身 反侦察 反追踪 数字足迹 社交媒体 预防性
[image] 关联	分身 ；[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2020年9月10日
[image] **Description**	操作安全性

好人的胜利在于，他们能成功地令坏人失败。

- Table of Contents

是否使用“真实身份”
匿名
持久性假名
集体身份
比较策略
真名
完全匿名
永久假名
集体假名
创建一个新的在线身份
1、创建名字和生活故事
2、可信的角色
1、工作 ——
2、技能和兴趣 ——
3、心理特征和态度 ——

4、语言指纹 ——
3、管理多个身份
商业社交网络平台
为每个身份使用不同的电子设备
最后

扎克伯格是个坏人，他的坏不仅在于他是全球最危险的监视资本家之一 —— 他利用偷窥我们每个人的一举一动来赚钱；并且，他利用他的知名度传播危险的价值观 —— 他说 ”如果你有两个身份，就是缺乏诚信的表现。”

您需要知道，扎克伯格之所以这样说，只因为 **Facebook** 希望将其用户打包成整齐划一的数据集供广告商使用。简言之，他为了出卖你，从而诱导你相信错误的价值观。

这和当权者所做的一样，他们告诉您 “实名制意味着正大光明”，和最臭名昭著的说辞 “你没什么可隐藏的”，都是在意图通过操纵您的价值观来为监视者提供最大程度的便利。 https://iyouport.substack.com/p/--dd7?utm_source=publication-search

[image]

如果多重身份让你想起政府信息战的水军操作，这不是您的错。这些水军的确采取的是多重身份，然而就像毒贩也使用Tor、基地组织的恐怖分子是最早使用 Telegram 频道的人、甚至中国外交部也在使用 Twitter …… 如果您因此而拒绝使用 Tor、Telegram 频道和 Twitter，想想看，这是谁的损失？

保护性措施不应该只保护坏人。作为想做些好事的好人们，您应该能做到比那些坏人具备更强的防御能力，只有这样才有希望击退他们。

[image]

返回：[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

互联网相比现实世界最有利的一面就是，您可以轻松将自己分解为多

种身份，比如个人身份、专业身份、娱乐身份、不同领域的互动身份等等；或者按照 “敏感” 等级分解为不敏感、中度敏感、高度敏感，等等。这取决于您的具体需求。

分身的好处在于，即便您的其中一个身份被追踪者瞄准了，即便该身份的保护性措施非常差，它也不至于连累您的其他部分身份。也就是说，追踪者不容易一次性将您的全部揭穿。

任何一个角色暴露了，您可以随时杀死它，重新再来。

[image]

激进社区用户请从这里进入：分身

分身对于政治敏感人士而言尤其重要。因为想要迫害你的人会将你的全面身份联系起来，您的政治立场和主张就会牵连到您的家庭、您的孩子、您的父母和恋人，您肯定不会希望发生那种事的。

这种行为被称为 doxing，中文叫它人肉，这已成为一种日益严重的威胁 —— 如果作为敏感人士，您的个人、专业和政治活动网络发生重叠，就无疑会给您以及您身边的亲朋及队友带来很大的危险。

请注意，并不是说您使用一个假名和虚假的个人身份信息就可以免于被追踪了，如果您在所有身份领域使用同样的假名和同样的虚构身份信息，也不难从中找到您的真实身份。因为您留给追踪者的线索太多了。

[image]

分身的要诀在于，分离出来的每一种身份之间都是完全不同的，尤其是，完全没有任何交集的，必须让每一个身份看起来完全独立，这样才能切断追踪线索。

本文将总结一些关于在线身份管理的基本知识，从分身意味着什么开始，直到管理多个身份的来龙去脉，以及如何使用某些工具、平台和设备，以补充您的在线身份管理。

首先要说的是，分身是一项建议，而非准入条件，您应该根据自己的需求作出最适合自己的判断。

是否使用“真实身份”

一旦您确定了自己的不同社交领域以及与之相伴的活动和网络，就需要开始考虑如何改善您与这些领域的互动方式了。

第一个要考虑的问题是，您是否要根据为自己确定的社交领域来区分您的个人身份，或者是否希望在每一个领域中都坚持使用您的官方名称和真面目。

这完全取决于您的具体需求，在这个问题上并没有“正确“或独特的答案，但必须说，这个过程和对您最终的选择无疑将影响到您在网络上的运营方式及其一切结果。

您可能想让自己的工作与您的合法身份或“真实“身份保持切合，因为这会让您的工作更具合法性；或者，您可能已经在该领域非常著名，由于各种原因，扭转这一点会出现问题。再或者，您可能认为您的行动主义应该是匿名的，您已经以一个虚构的身份确立了一定范围的影响力 …… 每个人都有不同的需求。

我们可以用2个例子来说明这点。

比如一位记者，如果她在写作中使用真实身份，她可能会有更多的知名度和工作机会。或者，她可能决定对自己的真名保密，用一个笔名（或“假名”）进行写作，这就意味着她采取了各种预防措施，让任何人都无法将这两个领域联系在一起。

这可能意味着她必须更加努力工作，以建立自己作为记者的公信力，一些潜在的雇主可能不愿意（或不能够）在不知道她的真实姓名的情况下为她的工作支付报酬，但是，将她的网络记者身份与真实姓名和

身份分开，对她个人安全来说是很重要的，也是足够有价值的，她需要为此付出一点努力。

再比如，一位活动家。如果他想用化名而不是真名，他应该考虑到自己可能会在现实世界中露脸，比如在会议上发言、参加示威活动、或参加小型活动。

他能不能把所有关于自己所做的一切行动主义相关工作的照片都保留到线下？如果不能，他在网上的假名将与他在任何现场照片中的脸中相关联，他的身份就暴露了。这可能最终会 “揭开” 他的网络活动家身份，使他最初选择使用化名的目标丧失作用。

如今的电子设备无处不在，以至于您可能都意识不到它们的存在（ BACK https://iyouport.substack.com/p/5e7 ）；从您的手机到各种所谓的智能家居，所有这一切玩意以及那些应用程序和功能每时每刻都在疯狂地吸取关于您的数据。在这情况下，要理解和保持对各种数据和元数据（即 “数字痕迹”）的认识，已经变得越来越困难了。

需要认识到这点，这意味着您曾经习惯于的谨慎模式需要 “与时俱进”，不断调整和深化。

考虑潜在的在线身份如何提高您的人身安全 —— 以及与您的私人和职业相关的其他人的安全 —— 准确评估风险、以及掌握安全使用各种类型的在线身份所需的技术技能，至关重要。

您还需要考虑在特定的情况下，您会使用哪种身份，它们之间绝不能发生错乱。

请回答以下这些问题，它们是您在评估在线身份时至少应该考虑的因素：

- 如果我的真实身份曝光，我的安全、工作或生计会受到威胁吗？

- 如果恶意者知道我参加了某些活动，我的心理健康或人身安全会受到影响吗？

- 如果我的真实身份被恶意者知道，我的家人或其他亲人朋友是否会受到任何伤害？

- 我是否能够并愿意安全地维护单独的身份角色？

请静下心来思考这些问题 —— 答案会根据每个人的需求的不同而有所不同。您所要做的就是，想得尽可能全面，而不是仅仅考虑最近的计划和此前才刚做过的事。把眼光放远点。

这些问题的答案意味着在考虑您的在线身份（或多个身份角色）如何影响数字安全性和隐私人权时需要应用的基本风险评估流程的要素。

在考虑不同的在线身份分离策略时，评估风险有助于更明确自己的选择和需求。

从完全透明到完全匿名，范围包括您认为需要并可能维护的多个独立身份，以便您安全地维护和完成工作。由于这项工作涉及风险，因此建议您尽力进行深入的风险评估，并在需要时寻求帮助。

[image]

匿名

匿名是指将您的身份和任何关于您的独特身份细节，完全隐藏起来。

这意味着需要保持您的真实身份与您所做的工作、活动和/或你所发表的任何意见，完全分开。

关于匿名，人权活动家 Vani 曾经写道：”我是一个经常使用社交网络的人。我就一系列的话题发表自己的意见。但我仍然是无脸无名

的”。

如果你不需要获得别人的信任，如果你可以信任的人很少甚至没有，或者当你不想让自己和生活中的其他人面临更大的风险时，匿名可能是一个不错的选择。

与下面的其他方案类似，它需要注意的是，您所创造的“数字痕迹”，就像前文讨论过的那样，它需要您非常小心、尤其是不要犯简单的操作性错误。

例如，对匿名的承诺意味着您必须非常有纪律地不透露自己的“真实IP地址”，类似于不透露您的“真名”。对于这一点，Tor 浏览器和可信的 VPN 可以成为您日常使用的关键工具。

[image]

可在本站“工具-Tools ”专题中搜索“VPN”，以查找您可能感兴趣的工具。

当您准备在进行某些在线活动时，匿名也是一个不错的选择，因为这些活动比您以其他类型的身份进行的其他工作和在线活动更敏感。

例如，当您在调查研究政府操纵的信息战时，或在可能被监控的在线环境中讨论容易被审查的内容或高度政治化的问题时，您可能希望保持匿名。

匿名也意味着使用其他类型的在线身份元素。如果你想与你不完全信任的人交流，或者你不愿意透露“真实”身份时，您可能想用化名建立一个一次性的账户，通过即时聊天或电子邮件与他们交流。

在网上匿名操作时，你可能也想用一次性的假名在博客文章或新闻网站上发表评论，或者建立一个一次性的昵称，以便在一次性的聊天中使用。

但是，完全的匿名性可能很难维持，尤其是当你长期创建大量的内容时。

你 —— 和其他知道你身份的人 —— 都可能会犯“错误”，会疏忽，并通过你发布的内容或元数据泄露出关于你的可识别性“数字痕迹“的几率会增加。

此外，在一些国家，匿名本身就可能是有风险的，因为在这些国家，匿名会自动被当局视为“危险信号”，当局可能会认为匿名用户试图隐瞒什么或做错了什么。他们就是这么愚蠢。

匿名也会让人感到孤独和孤立，这是一个心理健康问题，它不是听起来这么简单。长此以往的孤僻会威胁人的意志，您需要小心这点。
[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗

总之，请考虑周全。

你可以使用假名，但是，这些假名不应该在不同的网络或社交领域中反复使用，它们必须彼此独立；有些假名可能只用一次，之后便丢弃。正因为如此，匿名性与持久性假名不同。

持久性假名

持久性假名是指在一段时间内持续使用的假名。如上文所讨论的那样，有无数个理由让你想使用一个与你出生时的名字完全不同的名字。

请记住，使用化名意味着你仍然必须非常小心地将你的化名操作与你的个人生活完全分开，这意味着要密切关注在化名下创建的任何潜在的数字痕迹 —— 例如一张可以追踪到你的照片，或者你用真名做的电子邮件帐户、或论坛评论等等，或者透露你的“真实” IP地址。

所有这些都意味着，你必须真正确定这是你想做的事，并且你已经准备好做出所需的努力。

如果是这样，这里有一些需要考虑的事。

假名可以看起来像个人的名字，也可以是任意的短语，通常情况下，你会有完全的自由来创建假名，但是，也有一些服务机构会对使用假名或匿名身份的账号进行监视甚至封锁。

在撰写本文时，最著名的例子是 Facebook，它要求用户使用他们的“真实身份”（或 “真实姓名”），这几乎就是指你的法定姓名，或你通常被人熟知的名字（如昵称）。

避免这种情况的一个策略是使用姓名化名，这样您的账户就不会被 Facebook 等类似的服务自动挑出有问题。

持久的假名身份还可以提供匿名所不能提供的能见度，使您和您的工作在一段时间内获得在线声誉和关注度，并能与他人建立联系。

当然，成功地建立起网络声誉和与在线网络的联系仍将取决于基于信任的在线社区成员决定您是否值得他们的信任，这可以使您的在线声誉成为您的在线假名身份的关键因素。

您甚至可以选择向一些基于信任的网络中的一些人透露你的合法身份或 “真名”，或者不透露。任何可能决定将你的假名和与之相关的网络声誉与你的 “真名 “联系起来的决定，都是根据你的具体需求和背景做出的高度个人化的选择。

集体身份

另一种匿名的方式是通过集体匿名参与。

几个世纪以来，一些团体和志同道合的人们一直在以匿名方式参与历史性的抗议运动，或者以集体化名来创造出具有突破性的艺术作品和发人深省的行动。比如我们曾经推荐过的一部无政府主义剧集《La Casa de Papel》，这场行动的所有参与者彼此都不知道真实姓名，他们用全球的著名城市名来称呼彼此。

除了让成员们能够 “隐藏” 自己的身份之外，这些集体化名往往会从整个行为中产生一种近乎神奇的力量。

通过集体身份的匿名性可以转化为一些具体的活动和资源，从发布集体声明的私人群组或邮件列表，到共享的 Twitter 账号，都可以转化为具体的活动和资源。

虽然同样存在安全和隐私问题，但作为集体身份的一部分工作，可能意味着你背后有 “集体的力量”，如果你不想暴露自己作为运动的一部分的身份，这可以提供一个很好的选择。

但要注意的是，“集体的力量” 也可能导致结构性暴政。集体可能会选择做一些你不同意的事，或者是会让你处于无法接受的危险程度的事。仅仅是作为集体成员，就会增加你所经历的审查、监视和风险的程度。所以，如果你考虑以集体身份行事，在加入前要明智地选择，做好调查研究。

比较策略

至此，您现在应该对不同类型的网络身份有了更多的了解，知道了不同类型的网络身份有哪些、它们提供了什么、它们是如何重叠的，以及在使用这些身份时的权衡。

您可能已经想好了不同类型的在线身份如何以不同的方式与他人交流，思考什么样的策略适合您。

如上文所述，关键是要了解您的具体需求和情况在安全方面的利弊，

实施特定类型身份的要求，以及身份对你的具体风险程度所要求的技术能力。

您需要相对较强的技术知识和技能基础，才能安全地创建和管理这些类型的在线身份。入门训练建议从本站的S01系列开始。

选择将你的使用限制在某些平台上而不是其他平台上，可以帮助解决许多挑战，虽然不是所有挑战。建议您在可能的情况下，在选择使用一种或多种类型的身份信息之前，与其他在类似的高风险或敌对环境中使用过这些身份信息的人交流一下，作为研究的一部分，这是获得实践和了解这些身份信息的意义的绝佳方式。

以下是一个对比；

真名

- 风险：在线使用真名意味着家人、同事和其他人 —— 包括恶意者 —— 容易识别您的身份，并且您的活动可以链接回您的全部现实生活。

- 声誉：其他人可以轻松识别您的身份，因此获得声誉和信任更容易。

- 努力：不需要任何努力。

完全匿名

- 风险：很多情况下是有益的，但也比较难维护，需要较高得到的技能。

- 声誉：与他人建立联系从而获得信任和声誉的机会比较少，但并非没有，尤其是当您在一个组织中参与的情况下，比如匿名

者组织。每一位成员都能共享组织的声誉。

- 努力：需要很大的努力，因为需要大量的谨慎和技术知识。需要使用匿名化工具（例如 **Tor** 或 **TAILS**）

永久假名

- 风险：假名可能与您的真实世界身份产生关联，从而破坏您的防护。比如在操作失误的情况下。

- 声誉：永久的化名，其他人可以用来跨平台识别您的身份，这是获得声誉和信任的好方法。

- 努力：维护需要付出一些努力，特别是如果您还在其他地方使用真实姓名的话。

集体假名

- 风险：小组中其他人的行为可能会暴露您的真实世界身份；您需要与具备同等安全意识和操作习惯的人合作。

- 声誉：虽然这不是获得个人声誉的方法，但您仍然可以从集体的声誉中受益。

- 努力：尽管操作安全仍然很重要，但是与完全匿名相比，它需要的工作更少。

[image]

创建一个新的在线身份

就如我们一直在警告的那样，一旦一些东西进入了互联网，它几乎都会以某种形式在网上和私人服务器上持续存在。您可能会认为从社交网络平台和网络服务中删除某些敏感数据就足以保护自己，但请记住，元数据不能像删除内容那样容易，甚至没那么容易找到。

许多公司会删除你的账户，但可能会根据他们的政策和当地的法律，继续数据保留在他们的服务器上一段时间。而在你的整个生活中使用一个身份就会产生大量的信息，从而更容易对你进行 “人肉”。

避免这种情况的一个选择是留下一个旧身份，然后创建一个新的身份，或者（如上文所述）为你的每个社交领域创建不同的新身份。你也可以选择在某些领域仍然使用你的真实身份，而在其他领域使用新身份。

就像所有的安全和隐私策略及工具一样，当您没有面临直接的威胁时，您会更好地学习熟练使用这些防御措施。压力会影响您参与风险分析、安全规划和技能培养的系统化过程的能力。

所以，把安全措施作为习惯，而不是救急，才最有希望获得安全。

一旦你决定了想要尝试使用多种身份，并选择了您想创造什么样的身份（或角色），您可能需要考虑以下建议。

- 您应该为每个不同的角色身份慎重地选择社交联系人，严格避免与您用于不同活动的其他身份共享联系人。这将有效地创建独立的社交域，并拥有独立的账户、电子邮件地址、浏览器配置文件、应用程序，如果可能的话，包括独立的设备。

- 您的各种身份之间不应该存在任何联系，更不应该与您的真实身份存在任何联系。请记住，其中一些联系可能是完全下意识的，例如，当您使用真实的电话号码注册一个新的假名电子邮件帐户时，或在创建一次性使用的电子邮件时填写了一个持久性假名。这些都要不得。

- 创建额外的一次性身份是很有用的，因为，如果前一个身份被

泄露，您可以很容易地丢弃它。这些身份也可以为新认识的人创建（在适当的时候），在你把他们加入到一个更值得信赖的关系网络之前，也可以作为介绍性的档案来了解某人。

1、创建名字和生活故事

如上文所述，很多平台都有 “实名制” 政策，所以，如果你想用假名来使用这些商业社交平台，最好使用一个可信的名字和姓氏，而不是 “虚构” 一些看起来很假的名字和姓氏。哪怕您准备将该身份只用一次。

一旦您选定了虚拟角色的名字、姓氏和用户名后，您需要做一点研究，查看一下是否还有其他人使用过这个名字，即 采用我们曾经介绍过的用户名搜索工具：

[image] 在这里看到：https://t.me/iyouport/6861

您可能想要一个非常的独特的名字，也可能完全相反，您会选择一个非常大众的名字，以至于追踪者通过搜索后会产生大量的杂音，以便于您隐藏在其中。不论如何，这将根据您的具体需求来衡量。

然后，需要为这个虚拟角色创建一个故事，因为这样做可以使虚拟角色维护起来更容易。

这真的可以很有趣，也很有挑战性。如果你觉得特别有灵感的话，可以发明一个新的故事，或者根据一个 “已知” 人物的故事、一个你喜欢的小说中的虚构人物、或者采用一个 “集体身份”。

无论如何，当你创造一个身份时，你应该构思出一个 完整的虚拟人物，一个需要培养和发展的头像，才能成为可信的人物。

2、可信的角色

请注意，一个虚拟的角色或身份不可能只是一个名字、一个电子邮件地址和一系列的网络账户。如果您所有角色中保留了您所有的核心识别特征 —— 比如你的性别、职业、喜好，甚至是你的写作方式和用词 —— 那么最终肯定会有专业的追踪者可以把你的假身份和你的真实身份联系起来。

1、工作 ——

您的虚构角色所从事的工作应该和您的实际工作有所不同，但也不要差异太大，以至于您对该领域一无所知，那就很糟了。另外，您可能希望根据城市和国家/地区来更改工作地点。

2、技能和兴趣 ——

选择个人角色的技能以及角色所关注并撰写的主要主题时，应进行类似的考虑。

3、心理特征和态度 ——

赋予角色以深度的一个好方法就是，制造一些“弱点”，而这些“弱点”与您本人的真实弱点完全不同。所以，当角色受到攻击的时候，你可以一笑置之，不会受到伤害。比如说，如果你的幽默感很好，那么就可以尝试冒充一个完全没有幽默感的人。

4、语言指纹 ——

虽然比较高级，但您必须知道，可以通过“文体分析”来识别发言者的身份；如果他们有足够多的写作样本，就可以识别出某篇文章的作者。

当然这个方法很不常见，但是如果你担心这个问题，那就应该分析一下你的写作方式，分析一下你倾向于使用什么样的错别字、以及你倾

向于使用什么样的短语和句子结构。

你可以通过使用不同的写作风格来使任何潜在的分析复杂化，这可能涉及到你使用的单词、句子的结构、不寻常的大小写字母的使用，以及你通常不会出现的各种错别字。

如果您分身为多个角色，您可以为每个角色的写作方式创建一个简单的规则，并通过保存密码和每个角色的账号的登录信息来维持各个角色的不同特征。这当然是专门的技巧。

无论如何，您应该记住，在互联网上，你的每一个身份 —— 即使是那些与你的真实姓名相关的身份 —— 都是一个 “虚拟” 的身份，您完全可以决定在每一个身份中暴露出多少您想要的性格特征。在某些情况下，为你的 “真实” 网络身份创建一个有点虚构的角色甚至可能是个好主意。

[image]

激进社区用户请从这里进入：[image]语言指纹

3、管理多个身份

保持多重身份确实需要一些努力，就像大多防御做法一样，它需要您一些好奇心、耐心和注意力。

不必担心照顾不周，一段时间后，它就会像您在网上做的其他事一样成为习惯，最主要的一点是，要时刻保持警惕，以保持你的不同身份之间的完全分离，否则它们很快就会开始相互混杂。

开始的时候，您可以将不同身份角色记录下来，以帮助您避免出现将一个身份与另一个身份混为一谈的尴尬情况 —— 但一定要仔细考虑一下你在哪里保存这些笔记！不要让任何人碰到它们。

还有一些技术上的事可以做，下面会详细介绍。在任何情况下，请考

虑到这些建议集中于使用台式电脑的身份管理，可能并不总是适用于使用移动设备的相同活动。

可悲的是，移动设备具有太多的元数据和安全问题，更难控制和管理，这也是为什么它们一直被称为不安全设备的部分原因。

1、创建不同的浏览器配置文件，以伪装不同身份的浏览习惯。

2、在为身份创建新的电子邮件帐户或社交媒体帐户时，最好使用**Tor** 浏览器或 **Orbot** (对移动设备: https://securityinabox.org/en/guide/orbot/android).

如果需要电邮地址做联系方式，请考虑使用一次性电子邮件地址，该电子邮件地址仅用于该帐户。

但需要注意，您选择的电子邮件提供商必须不能同时收集和显示新的 "一次性" 电子邮件帐户和您的真实身份之间的联系 —— 例如，当你的主要 "真实身份" 电子邮件帐户中的一个已经链接到 Chrome 浏览器时，试图通过 Chrome 浏览器再创建一个一次性 Gmail 帐户，是几乎不可能的。

考虑使用你通常不会使用的其他电子邮件提供商来制作一次性账户。

3、写出并建立你在不同身份的账户中 "登入和退出" 时所采取的 "基本清理" 步骤。

这包括注销账户、删除 cookie、不要让浏览器保存密码等等。显然，您还需要为每个账户管理不同的密码，所以强烈建议您使用 Keepass 等密码管理器工具来管理不同的密码。

如果你有资源和动力，你可以根据设备或操作系统来分离你的身份。例如，这可以包括使用虚拟机。这个选项可以是一个非常有用的方法来使用和管理你的各种账户。

无论选择哪种方法，都应尝试使流程尽可能地例行化，以使其成为您可以在工作流中管理的部分。

商业社交网络平台

在选择使用任何社交网络平台之前，无论您打算使用哪种身份，都应询问一些基本的安全和隐私问题，如下：

1、它是否为网站的所有使用提供了加密连接（https），而不仅仅是在登录期间？网站的加密是否存在任何问题？

2、根据平台的最终用户许可协议（EULA）、隐私政策和/或数据使用政策，您的内容和个人数据是如何被处理的？与谁共享或可能出售给谁？

3、该平台为用户提供了哪些隐私选项和功能？比如说，你可以选择与少数人安全地分享你的视频，还是默认所有的视频和其他内容都是公开的？

4、是否知道这些服务器的地理位置？它们属于哪个地域（因此也是法律上的）管辖范围？该公司在哪里注册？这些信息与您的活动和信息的隐私性和安全需求之间有什么关系？

现在，当您考虑制作一个单独的身份并将其发布到商业社交网络平台上时，还需要采取其他预防措施，比如：

1、首先重要的是，不要暴露你的“真实”IP地址，所以建议使用可以屏蔽你的IP地址的工具，如Tor浏览器或可信的VPN来连接到这些平台。

2、在为新角色创建社交网络账户时，请使用你为该角色创建的唯一的浏览器配置文件（如上文提到）。一定要检查平台的隐私设置，这样你就能知道谁能看到你发布的内容，谁能与你联系，谁能用搜索查

找你，以及你的联系人能看到和做什么（例如，他们能在图片上标记您吗？）

3、仔细考虑您提供的个人资料，要记住，这些资料是公开的，所以要考虑你想传达的信息。

4、确保每一个角色的联系人与您的其他角色身份之间不要重叠，不同的身份不要互“关注”！

如果有人想揭开其中一个角色的面纱，他们首先要找的就是这个账号跟随谁、谁在被跟随。出于同样的原因，您应该严格避免将一个账号发布的帖子或其他内容用另一个账号转贴。

5、为了让您的身份角色看起来像不同的人，您可以在一天中的不同时间段从您的不同账号中发布不同的帖子。一些社交网络平台允许用户安排自己的帖子的发布时间，也就是定时发送。

6、从你的假名角色中关注其他可能被合理地认为是该角色真正所有者的人，这可能是个好主意。把追踪者带偏。

为了进一步拉开你的真实身份与假身份的距离，你也可以在假身份下写下关于你没有参加的活动的帖子（并在 Twitter 上用标签），特别是当这些活动的发生地点离你很远的时候。

发布一些看起来就像是你暴露了身份的帖子，然后删除，这样做也会很有趣，这样可以进一步迷惑那些可能试图揭穿你的身份的人。

7、如果你使用的是带有GPS功能的手机，大多数社交网络平台都会在能显示位置的地方显示你的位置。这个功能一般是在您使用支持GPS的手机与平台互动时提供的，但您的电脑所连接的网络也可能提供位置数据。

仔细检查您的设置—尤其是在照片和视频分享网站上，确保您的物理位置和其他元数据不会被收集并与您分享或发布的媒体内容共享。

8、如果您通过手机APP访问社交平台，最好为每个独立的账号使用不同的**APP**，以免误将东西发布到错误的账号上。

[image]

为每个身份使用不同的电子设备

数字安全的方法有很多，但最现实的方法之一就是“隔离式安全”，它假设所有的安全措施都有漏洞，因此重点是：通过防止可能的攻击者访问需要安全保护的 “整个系统” 来减少伤害。

这就是使用多个在线身份相互隔离的策略的基础思考方式 —— 它将一个难以防御的单一目标（你的 “真实身份”）转化为多个目标（你的各种在线身份） —— 如果操作正确的话，它可以是很有效的，但这完全取决于您的具体情况和您所要创建的安全类型和深度。

归根结底，这取决于您真正认为你的 “对手“是谁，以及您认为他们有什么样的能力。

您如何在网上向外人展示您的形象，与您如何向间接访问您的设备或您使用的服务的人展示您的形象是非常不同的。如果你的工作环境中，你希望对你的设备和服务有更大的控制权，那么有一个技巧就是：将这一策略从独立的、孤立的在线角色扩展到您使用的设备上。

大多数人在同一设备上使用相同的操作系统来创建、使用和管理所有的在线身份，因为人们通常只能使用一台电脑和一部手机。

由于浏览器和应用程序可以进行独特的 “指纹识别” ，当您使用不同的在线身份时，就必须采取额外的步骤来 “显示” 不同的在线身份。

其中一个方法是改变您使用的浏览器，并为每个在线身份创建和保存单独的浏览器配置文件。

请注意，犯错的概率可能有点高。例如，你可能会不小心使用“真实”身份分配的浏览器配置文件登录到了一个假名账户，这就会留下明显的元数据，与你通常使用的浏览器配置文件相比，这些元数据似乎不寻常，如果有人在你登录时密切关注并捕捉到了你的浏览器数据，就可以将假名账户与你的真实账户联系起来。

你还可能被恶意软件感染，使攻击者能够监控你在网上所做的一切，包括使用你的许多精心制作和管理的假身份来监控你的所有活动。

请不要自责，每个人都有疏忽的时候，我和您一样不可能采取7*24的紧绷状态。但这些疏忽的确非常危险，它们会导致您前功尽弃。

为了减轻这些风险，你可以为你的每个在线账户（及其各自的社交领域）使用不同的设备，这样就可以减少潜在的间谍软件或人为错误可能造成的伤害。

然而，我们大多数人都没有这样的资源。因此，一个廉价的（通常也是免费的）选择是：在您的主电脑上使用不同的操作系统，比如使用像 Tails 这样的 GNU/Linux Live 发行版，或者创建“虚拟机”，在你的主操作系统内运行。

虚拟机(VM)可以被描述为一个模拟的计算机，它有自己的操作系统，以软件的形式运行在你的物理计算机上。你可以把虚拟机看成是计算机中的计算机。

在虚拟机中打开不受信任和潜在的有害附件，还可以帮助您与主操作系统“隔离”，以避免整个系统受到潜在的恶意软件感染。

这里提出的三个工具 —— **Tails**、**Whonix** 和 **Qubes OS** —— 都可以为您提供额外的保护，让您无需使用多台电脑就能管理备用身份的独立操作系统，并且可以成为确保您在使用其他在线身份相互隔离的情况下不会暴露真实身份的强大工具。

更棒的是，这些解决方案都是免费的、开源的 **Linux** 发行版，可以最大限度地保护用户的隐私和安全。

Qubes 可以将您在计算机上做的事安全地隔离在不同的虚拟机中，这样，如果一个虚拟机受到攻击，其他任何事都不会受到影响。

这样一来，你就可以在一台物理计算机上做任何事，而不必担心一次成功的网络攻击会危害到您的整个系统、泄露你的各种身份之间的所有连接。

如果您想把所有的活动都放在自己的电脑里，而不需要安装其他任何东西，那么 Qubes OS 就是个不错的选择。

请注意，您始终不应该把这些技术工具看出灵丹妙药，操作安全始终是第一位的 —— 人是最大的漏洞。请尽可能将操作安全形成习惯。这些工具可以使遭受攻击的可能性降至最低，您值得花点时间去熟练使用它们。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

最后

我们中大多数人都希望在网上与他人安全地进行交流和组织。所以，如果您能在网上创建和维护安全、可信的社区，让那些有共同目标、观点或想法的人进行更广泛地交流、支持和对话，您就可以构建有效的避风港。

从个人防御开始，到形成组织的防御，当您可以协助身边的队友形成同等的安全意识时，您和大家就可以开始自由地做想做的事了。

防御是一切的基础，如果您能在不自由的世界里为自己和组织创建一片自由空间，您的存在本身就已经是有效的反抗。平安顺利！

[image]
[image]

为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式

[image] 关键词	对抗性思考方式 开源情报 数字安全 自检
[image] 关联	[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ ；🔍开源情报
[image] 创建时间	2020年9月25日
[image] **Description**	操作安全性

本文是希望您对开源情报有一个比较客观的了解，关于它能做什么、不能做什么、以及最好用来做什么的认识。尤其是对于生活在警察国家中的人们来说，只有当您能够了解警察和间谍是如何抓捕公民的时候，才能作出最有效的防御。

- Table of Contents

互联网上的几乎一切都可以是开源情报，也可以都不是开源情报
为什么开源情报在这个时代再次被重视
他们可以是：
他们还可以是：
我们为什么要采取开源情报
在中国：近20年的在线数字镇压
KIS在自我介绍中描述它自己可以：
KIS在自我介绍中描述它的目的是：
KIS 在其介绍中表示：
KIS 的介绍中还强调该监控系统的诸多“优势”：
社会反应

开源情报的优势
开源情报的弊端
1、信息战地缘政治
2、“开源”不是全部
3、与隐私倡导相悖
我们对开源情报的使用
最后

[image]

我们看到越来越多的中国读者开始对开源情报产生兴趣，这真是令人兴奋。

但是，我们希望能首先完整解释下这件事，关于IYP为什么要采取开源情报，这事关对该反抗形式的理解和定位。

互联网上的几乎一切都可以是开源情报，也可以都不是开源情报

“开源” 这个词意味着您可以找到的任何东西。不论您的挖掘有多么深刻，它都符合 “开源” 的概念。甚至包括骗，都可以。比如采取袜子木偶账户接近目标人以此获得 “朋友” 级别的知情权限、甚或使用各种办法套取对方说出[暴露]可追踪的线索。

但 “情报” 这个词意味着，您的最终调查产品必须有可操作性。也就是说，它必须能对行动部署、目标推进、审议定夺、决策制定 等程序具备指导意义。

也是为什么我们说 https://web.archive.org/web/20200819195129/https://www.iyouport.org/%E5%88%86%E6%9E%90%E8%80%8C%E4%B8%8D%E6%98%AF%E6%94%B6%E9%9B%86%EF%BC%8C%E6%89%8D%E6%98%AF%E6%83%85%E6%8A%A5%E7%9A%84%E7%81%B5%E9%AD%82%EF%BC%9A%E5%A1%91%E9%80%A0%E8%B6%85%E5%BC%BA%E8%AE

%B0%E5%BF%86/

[image]

[image]

每一种行动的前提都是情报，行动策划者必需能够获得与手头的调查或事件有关的及时、可靠和可操作的情报。

没有情报的行动是不应该存在的，那将意味着盲目和必输无疑。您能想到的任何行动都是如此，不论是正义的还是邪恶的。情报是成功之源。

目前您能在互联网上看到的开源情报报告大多是不完整的，因为它们是以训练为目标的演示，也因此，它们也大多突出了整个开源情报调查中最关键的/难度最大的那些部分。

开源情报这个概念听起来很高大上，其实它的支柱就是每一个使用互联网的人都熟悉的东西 —— 搜索。只是，这里的搜索和普通的搜索不同，它更为深入、范围更广、更有目的性、更专业和复杂；最重要的是，它有一个确定目标，一切操作都为了这个目标而努力。

为什么开源情报在这个时代再次被重视

我们曾经在 https://web.archive.org/web/20200205001443/https://www.iyouport.org/%E7%A7%91%E6%8A%80%E5%A6%82%E4%BD%95%E6%94%B9%E5%8F%98%E6%83%85%E6%8A%A5%E4%BA%A7%E4%B8%9A%EF%BC%9F-%E6%8A%80%E6%9C%AF%E5%92%8C%E9%97%B4%E8%B0%8D%E7%9A%84%E6%9C%AA%E6%9D%A5/ 一文中解释了这个问题。大规模监控已经损伤所有人的活动自由，这其中也包括需要严格隐藏身份的政府间谍 —— 尤其是那些跨国行动的间谍，这是他们搬石头砸脚的最突出笑话之一。

于是，人工情报在数字技术监视时代已经严重受限。同时，公民反抗的崛起（如 PI、ACLU 等权利组织）、以及 https://start.me/w/

MnlJ8o 努力，虽然信号情报的获取虽然仍在很大程度上不受限制，但是只要能被曝光，间谍行为的后果会让政府很麻烦。 BACK https://medium.com/@iyouport/%E8%B0%B7%E6%AD%8C%E5%9C%B0%E5%9B%BE-%E6%98%AF%E6%AF%94%E8%A9%B9%E5%A7%86%E6%96%AF%E9%82%A6%E5%BE%B7%E6%9B%B4%E6%A3%92%E7%9A%84%E9%97%B4%E8%B0%8D-9df6eb4f6527 。

在这种情况下，开源情报便成为了最具生命力和有效性的情报获取途径。当然，这是对当权者而言。

因为它完全合法（至少目前为止在任何国家都是如此），并且操作极为宽松，尤其是，它可以具有强大的侵入性能力（因为如今几乎所有人都把自己放在互联网上了，其中为数不少的人甚至在线曝光了自己的一生）。

易于追踪监视就是这个互联网的工作方式，正因此，它为开源情报提供了一个前所未有的巨大金矿。

[image]

延伸：https://iyouport.substack.com/p/305?utm_source=publication-search

所有人都在这里挖掘。

每个人都有不同的目的。

他们可以是：

- 对真相和知识好奇的网民 BACK https://iyouport.substack.com/p/6f5?utm_source=publication-search；
- 用行动抵制政府信息战操纵的活动家组织 BACK https://

iyouport.substack.com/p/lr-2?utm_source=publication-search；

- 致力于揭发暴行的人权捍卫者 ；

- 信仰知情权为民主根基的公民调查人员 https://medium.com/@iyouport/%E8%B0%B7%E6%AD%8C%E5%9C%B0%E5%9B%BE-%E6%98%AF%E6%AF%94%E8%A9%B9%E5%A7%86%E6%96%AF%E9%82%A6%E5%BE%B7%E6%9B%B4%E6%A3%92%E7%9A%84%E9%97%B4%E8%B0%8D-9df6eb4f6527；

- 与虚假信息作战的事实核查人员 https://web.archive.org/web/20200627194353/https://www.iyouport.org/%e5%bc%80%e6%ba%90%e6%83%85%e6%8a%a5%e5%92%8c%e5%8f%96%e8%af%81%e5%ad%a6%e5%a6%82%e4%bd%95%e5%af%b9%e4%bb%98-%e6%b7%b1%e5%ba%a6%e9%80%a0%e5%81%87%ef%bc%9f%ef%bc%88%e6%9c%89%e5%be%88%e5%a4%9a%e8%a7%86/；

- 试图揭露诈骗行为的正义人士 https://medium.com/@iyouport/%E6%BC%94%E7%A4%BA-%E5%AF%B9-elon-musk-bitcoin-%E8%AF%88%E9%AA%97%E7%9A%84%E5%BC%80%E6%BA%90%E8%B0%83%E6%9F%A5-osint-394e6f8bbe6a；

- 寻找失踪儿童的NGO；

- 揭露大企业内幕的调查记者 https://iyouport.substack.com/p/lr--4f2?utm_source=publication-search；

- 追踪数据泄露和网络攻击的安全技术人员 https://web.archive.org/web/20201126011404/https://

www.iyouport.org/%e5%a6%82%e4%bd%95%e7%90%86%e8%a7%a3%e5%99%aa%e9%9f%b3%ef%bc%9a%e8%ae%a9%e5%bc%80%e6%ba%90%e5%a8%81%e8%83%81%e6%83%85%e6%8a%a5%e6%9b%b4%e7%ae%80%e5%8d%95/

- 以及其他正义之士 ……

他们还可以是：

- 为完成“抓人指标”不惜余力的网警；
- 致力于将任何反抗行动扼杀于摇篮的维稳部门；
- 为了钱什么都干得出的骗子；
- 正在策划入室抢劫的犯罪分子；
- 正在钻研入侵目标的骇客；
- 随时准备恐吓和伤害您的人肉狂 ……

那么，IYP是上述的谁？

其实谁也不是。

[image]

我们为什么要采取开源情报

IYP自2016年左右开始关注政府监控并间断性地讲述安全知识，尤其是讲述在线监视所带来的危害的相关信息。但是效果一直不理想，进

展缓慢。

反馈主要有两个倾向：

1、一些读者（尤其是对技术不擅长的读者）开始将危险无限放大，以至于倾向于实施更为苛刻的自我审查，甚至审查周边人 —— 由于中国有一个臭名昭著的“群主承责”规定，即 一个在线群组中如果出现被当局不喜欢的信息和交谈，组织该群组的人将承担责任。

2、另一些读者则是不为所动，感觉自己平庸的生活“没什么可担心的”（这点也是很多国家都存在的现象）。 BACK https://iyouport.substack.com/p/--dd7?utm_source=publication-search

这期间我们多次调整传播模式和表述方式，可惜一直没有什么起色。

于是2018年开始，我们采取了更为激进的策略—— 用演示追踪来提醒隐私保护的重要性和方法。即，让人们直观地看到政府和恶意者会怎么做。

这被称为对抗性思考方式。

它的原理很简单，类似于您在学习英语的时候老师强调的“词源学 Etymology”，也就是说不再死记硬背，而是去了解这个词是怎么来的，这样您就可以不至于拼写错误。

知道它是怎么来的 —— 这点适用于大多数学习。当然也包括安全知识。

就如，

- 当人们看到“https://iyouport.substack.com/p/e35?utm_source=publication-search”时，在下一次上传照片之前就不会仅仅满足于遮住脸部了；

- 当人们了解到https://web.archive.org/web/20200810180304/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E6%8C%96%E6%8E%98%E7%9B%AE%E6%A0%87%E4%BA%BA%E7%A4%BE%E4%BA%A4%E5%85%B3%E7%B3%BB%E7%BD%91%EF%BC%9F-%E8%BF%9E%E9%94%85%E7%AB%AF%E5%88%A9%E5%99%A8/ 曝光了自己的私密交往时，就会多一些小心以更好地避免在真正的行动之前被连锅端。

- 当人们知道 https://web.archive.org/web/20191012034652/https://www.iyouport.org/%E5%A6%82%E6%9E%9C%E5%8F%AA%E7%9F%A5%E9%81%93%E4%B8%80%E4%B8%AA%E7%94%B5%E8%AF%9D%E5%8F%B7%E7%A0%81%EF%BC%8C%E4%BD%A0%E8%83%BD%E6%8C%96%E5%87%BA%E5%A4%9A%E5%B0%91%E6%9C%89%E6%95%88%E4%BF%A1%E6%81%AF/成为任何追踪者的利器时，就不会再通过不安全的网络分享手机号了（曾经这种做法特别普遍）；

- 当人们看到可以科学地识别并有可能追查 trolls 背后的人时（https://web.archive.org/web/20200509043106/https://www.iyouport.org/%E7%BD%91%E7%BB%9C%E6%B0%B4%E5%86%9B%E5%A6%82%E4%BD%95%E8%AF%95%E5%9B%BE%E5%BD%B1%E5%93%8D%E9%80%89%E4%B8%BE%EF%BC%9F-%E4%B8%80%E4%B8%AA%E8%B0%83%E6%9F%A5%E6%A1%88%E4%BE%8B%EF%BC%8C%E8%A7%82%E5%AF%9F/），“全面拉黑”的传统建议就不再吸引人了（全面拉黑只会让异议人士的圈子越来越小，主要原因是，人们经常错误地拉黑不同意见者，而非真正的trolls）；

- 当人们看到一张自拍照就可以准确定位地理位置、甚至曝光家庭住址时（https://web.archive.org/web/20200926160658/https://www.iyouport.org/%E5%8F%AA%E6%9C%89%E4%B8%80%E5%BC%A0%E7%85%A7%E7%89%87%EF%BC%8C%E8%BF%BD

%E8%B8%AA%E7%9B%AE%E6%A0%87%E4%BA%BA%E7%9A%84%E9%95%BF%E9%80%94%E8%A1%8C%E8%B8%AA%EF%BC%9A%E6%A1%88%E4%BE%8B%E6%BC%94%E7%A4%BA/ ），再上传任何照片都会至少反思一下 “追踪者会利用它来做什么” BACK https://iyouport.substack.com/p/--166；

- 当人们发现一些简单的搜索和有效的思考方式能够鉴别很多虚假信息并回答最想要知道答案的具体问题时 ……

这种方法被证明在一定程度上是有效的。正如这位读者所言：

[image]

在中国：近20年的在线数字镇压

中国当局对互联网开源情报的使用甚至可以追溯到近20年前—— 臭名昭著的网络舆论监控技术公司中国厦门的美亚柏科，成立于1999年。

随着美亚柏科的所谓 “成功”，其他公司也相继开始投入 “网络舆情分析” 的产业。比如中国深圳的 KIS（Knowlesys Intelligence System）。

网络舆情分析只是社交媒体情报的委婉说法，前者而不是后者这一概念在中国已经流行多年，它更为含糊、并具有误导性，使人们误解其仅仅是 “分析”，从而有意掩盖了监控的严重后果。直到不断有社交媒体用户被警方传唤、甚至被逮捕、被判刑。

以 KIS 为例，这家位于中国深圳的公司是一家标准的监控公司 —— 使用开源情报追踪任何其 “客户” 想要的人和事物，并提供多种情报产品。

[image]

他们的自我介绍是："基于全球领先的开源情报提取技术；从社交媒体（推特，**Facebook**，**Youtube**，**Insatgram ...**）和传统网站（论坛，聊天室，新闻**....**）中挖掘大量信息，并通过自动分析和手动处理将其转化为可操作的情报。

KIS在自我介绍中描述它自己可以：

- 监控与相关城市或省相关的所有信息，尤其是所谓的负面信息；
- 后续处理 —— 联系目标网站管理，采取应对措施，毫不拖延。就是删帖；
- 实时监控 Twitter / facebook、 youtube，bbs，博客，论坛；
- 监控聚焦QQ /微信群组的聊天内容
- 跟踪某个主题或作者的所有信息 ……

KIS在自我介绍中描述它的目的是：

■ 消除或尽量减少偶然的负面信息对相关省/市和政府官员形象的不利影响—— 洗地；

■ 识别和理解目标省/市的舆论，解决刚出现时的冲突—— 维稳；

■ 识别网络内容的威胁（例如泄露机密信息）—— 封口；

下图是该监视系统的三个子系统构图。

[image]

KIS 在其介绍中表示：

- 政府用户可以在该监控系统中自行添加新闻网站、论坛网站等监视目标网站；
- 并且，谷歌、**Twitter** 和 **Facebook** 都是已经内置的监控目标；
- 自动提取子系统还可以监控基于应用程序的网络聊天室；

自动提取子系统的全方位监控功能如下图所示：

[image]

KIS 的介绍中还强调该监控系统的诸多“优势”：

- 在中国国内收集被GFW封锁的外国网站、收集受源IP和访问频率限制的网站、以及自动收集代理**IP**地址，无需进一步配置。
- 设置关键字后，一旦收集到的内容中出现一个或多个关键字，就可以将记录发送到相关的短信接收器，进行无人值守的实时监控 ……

作为服务于政府的开源情报公司，**KIS**成立于**2003**年（美亚柏科成立于**1999**年），也就是说，在近**20**年的时间里中国当局一直在至少使用上述方法监控全网。

加之，中国总理李克强在2015年对所谓的 “互联网 + ” 的大力推动、对云计算、大数据、物联网等现代技术在政策方面的支持 —— 政府设立了400亿元新兴产业创业投资引导基金—— 相关监视技术供应商得到了更加快速的发展。

同时期开始，大数据和云计算技术成为多家大型网络公司的开发重点 —— 作为网络维稳的 “必要工具”。

以美亚柏科为例，云计算的作用主要是结合大数据方面做舆情监测，项目可提供给省级及以上的政府机构，包括公安、国安等部门，财报显示这是该公司2013年的重点项目，是2014年收入和利润的重要来源。

其次是网络监控，主要表现在舆情监测和证据固定等方面，美亚柏科不仅是技术的开发、提供者，而且是具体服务的执行者，该公司还负责 “舆情分析师” 培训。

其三是信息收集和分析，也就是大数据服务，可以提供给其他部门。最后，其他服务主要是系统和设备，各种数据采集、存储、传输等。这部分在美亚柏科公司官网中 “产品和服务” 一栏里面有写明，存在与政府当局较为密切的关系。

已知的同类监视公司不仅包括KIS，还有 邦富 （互联网舆情监控及分析系统、GIS舆情预警系等）、 启明星辰 （互联网行为监控、防火墙等）、 浪潮 （云计算、大数据、服务器）等等……

公安IT系统建设是极早的，2006年就已拥有了成熟的数据中心，而公安几乎和所有行业在数据层面都有密切交互。

浪潮信息副总裁彭震曾特别提到：“浪潮服务器已经在80%省份公安系统中得到广泛使用，浪潮的大数据产品早已走入公安系统”。

浪潮信息云产品部副总经理李忠旭曾表示：“以全国八大信息库为基础，以五大案件（人、地点、机构、物品、案/事件）要素为基本信息分类，以 ‘大情报系统’ 建设为突破口，公安可以很快建立起新一代大数据云应用平台。这其中，面向海量非机构化数据的存储和分析处理；面向海量数据的在线查询；面向海量关系型数据的分析挖掘的浪潮大数据一体机和相关解决方案提供商将能提供更多帮助。”

很明显，这是一套完整的网络数字镇压技术支持。

从讯息的挖掘、监控、分析到共享，大数据和云计算技术使政府相关

部门具备了更强的维稳实施能力，可以更快速洞察线下维权抗争事件的发生并快速做出反应，全面监控收集庞大的数据资源，优化了维稳系统，线上线下相结合，“互联网＋” 数字镇压O2O（线上到线下模式）。

[image]

社会反应

最初的几年里，人们仅仅是“知道”有谁因网络言论而被捕—— 是的，中国当局并不刻意掩盖这点，相反，他们默许受害者及其家人和朋友通过互联网传播被捕的消息，以此来激发更大范围内的恐慌和自我审查—— 却很少有人会思考关于 “当局是如何发现我的真实身份的？”

由于寒蝉效应格外明显，大众倾向于将政府视为无所不能和至高无上，以至于保护性措施的推动在同期遭遇了严重的阻力，人们会说 “没用的，他们（政府）能做到一切”。

当这一想法随着时间的推移被深化时，它就变成了 “莫谈国事”。在线中文群组多如牛毛，人们用来拉拢彼此之间的感情，但几乎没有任何群组能就一个主要/关键社会议题展开有效的讨论，是的，包括加密群组。

来自中国的联系人在通过加密通信应用和匿名邮箱与我们联系时，继续使用只有我们和他才能懂的暗语。因为他也预设了政府无所不能的前提，他保持了自己在任何情况下都使用暗语的习惯。

“他们（政府）总有办法知道你是谁”，人们这样说，从而对任何匿名策略建议表示怀疑。

尤其是中国的异议人士、记者和活动家，在中国这些群体普遍对技术陌生，为了支持自己的坚定，其中大部分人将 *主动实名* 视为勇气的象征，从而拒绝任何化名掩盖真实身份的措施建议。

当然，也有一些现实的理由，比如记者和人权律师，他们需要在线实

名，以“可靠的形象”联络需求者；他们会在线发布大量的个人信息，比如照片、视频、联系电话、甚至分享实时的地理定位。

但这不是一成不变的。逐渐的，人们的思想开始转变，尤其是在越来越多的网络用户被传唤、被恐吓剥夺权利、甚至被逮捕之后，包括身在海外的留学生。传闻开始怀疑例如 Twitter、Facebook 等美国平台与中国政府合作暴露用户的私密信息。

并不排除这种可能性，就如美国公司帮助中国构建的那些监视技术一样，不为人知的暗地合作恐怕永远都揭露不完。但是，对于绝大多数言论罪的案例来说，事实上当局完全不需要这些美国寡头公司的配合，因为受害人几乎没有认真采取保护措施。不仅当权者，任何人都不难追踪到他们的真实身份。

为了能够实现最有效的防御，我们应该将精力用在最有针对性的位置上。

这就是我们采取开源情报的主要目的：对抗性思考方式。

开源情报的优势

当然我们承认，对抗性思考方式并非开源情报的常规用例，该社区中多数参与者均致力于[期待于]为情报机构服务（期待作品积累以丰富简历进而寻求相关工作）。也因此，其中很多作品的主题侧重于地缘政治、维稳、贴近政府议程。

这绝非我们想要的，相反，是我们致力于防止的东西。于是，这就出现了一个 “捷径” —— 开源情报社区的很多演示来自于接受过专业培训的人员，或其本身就是培训师，于是这些内容能在一定程度上帮助防御者捕捉到追踪者的思考方式。

如上所述，开源情报作为公民反抗工具的用例非常多，它可以是直接行动的一部分。

比如：

1. 作证。联合国已经将开源情报调查报告作为确定侵犯人权行为的证据；

1. 事实核查。操纵公民的认知就能操纵民主，这就是为什么当权者愿意一掷千金投入信息战交易，黑公关产业风靡全球。核实和揭露虚假信息对民主维护至关重要。 https://iyouport.substack.com/p/--c32?utm_source=publication-search

1. 信息战。你看到的“民意”究竟是不是真的？是谁在背后试图分化反抗者社区让人们处于无意义的争吵中一事无成？曝光信息战网络，及时排除诱导和操纵，避免活动家偏离目标。

1. 寡头公司的内幕。对于政治旋转门的挖掘将帮助您理解深层局势、并制定更有效的反抗计划。 [image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

1. 此外，揭露诈骗、寻找失踪人口等等，都是社区自治的有效工具。 https://iyouport.substack.com/p/07c?utm_source=publication-search

开源情报的弊端

和大多数工具一样，开源情报有其天然的局限性。

1、信息战地缘政治

开源情报调查的确可以作为揭露信息战的工具，但是，它本身也可能被作为信息战的工具。而且已经在这样做了。

下面这两张图您一定很熟悉：普京撸管、奥巴马袭胸 ......

[image] [image]

这些图像还有很多，它们是在试图告诫大众：在完全真实的信息中只需要遮盖住一小部分，就可以形成误导性。

如果您熟悉企业媒体的宣传，一定对这种操作不会陌生。但您知道吗，同样的方法完全可以用在开源情报产品中 —— 只需要着眼于一个局部进行调查，其结果就是令其具有宣传价值，而非认知价值。

等下，每一步调查都有清晰来源、逻辑严谨的开源情报调查产品也能变成信息战武器？的确是这样，尤其是它在地缘政治斗争中的使用 —— 竞争双方都在努力证明自己才是对的。

比如在冠状病毒引发的中美关系嘴炮大战期间，如果您采取开源情报挖掘社交媒体上有多少信息战水军致力于将病毒来源归因于中国，并可视化这一宣传战网络，您可以做出一份很棒的开源情报调查报告。而且完全真实。

但是，如果您再研究一下究竟有多少水军致力于将病毒来源归因于美国 ...... 再一次，另一份完全真实的调查报告就诞生了。

那么，究竟是谁在抹黑谁呢？

这两份报告并没有指导意义，但是如您所知，它们却能形成有效的宣传 —— 当您只发布其中一份的时候。

2、“开源”不是全部

开源调查顾名思义它就首先局限在“开源”方面。比如以色列的例子。

去年，一个以色列监督组织表示，在选举之前，他们发现了一个社交媒体机器人网络，专注于传播支持总理本杰明内塔尼亚胡的信息。

他们在报告中写道，他们发现了数百个假账户，这些账户传播的信息都是支持内塔尼亚胡的利库德集团，并抹黑他的对手。利库德否认了这些指控。

这是个众筹资助的调查小组，是独立的观察员。这份报告引起了很多关注，但结果却是，引来了内塔尼亚胡政府的倒打一耙。

他称这是一种基于 “虚假调查” 的媒体的 “虚假诽谤”。

“几乎所有的例子都证明是真正的人。他们有一个名字，他们有一张脸，他们有家庭，最糟糕的是：他们有自己的意见。他们是独立人士，“ 内塔尼亚胡说，“其中没有一个是假的。”

甚至，该报告中提到的一位 Twitter 用户 Ziv Knobler 在接受以色列陆军电台采访时表示，“没有任何组织。我们是一群相信本杰明内塔尼亚胡的人。“

“我们表达了个人意见，而不是代表一个组织，”Knobler 说。 “我们与利库德集团完全没有联系。”

最终，如您所料，这份原本很漂亮的调查，没能对抵制信息战带来任何帮助。内塔尼亚胡成功连任。

这里的问题在于，调查人员没能将该宣传战网络与内塔尼亚胡及其党派联系起来；也就是说，没能找到该水军网络受雇于谁的证据。

要做到这点并不容易。除非能找到资金流向，否则无法证明受雇。如果不能证明受雇，那么就必须接受其作为 “民意” 的结论 —— 不论其有多愚蠢和荒谬。别忘了，如今的信息战中已经开始大量使用真人，而非机器人水军。

[image]

延伸：https://iyouport.substack.com/p/lr-2019?

utm_source=publication-search

开源情报的确可以做到追踪资金流，如果交易通过互联网的话。但对于现金支付可能就无能为力了。更何况在很多国家，信息战组织是在当权者暗示利益的情况下展开的，比如暗示参与将有利于就业、求学、升职 …… 就如您在中国听闻的那样。

开源情报作为一个步骤是非常有用的，那就是揭露信息战的存在；但是，必须跟进其他来源的情报以证实操纵背后的主导者，才能达成目标。

再比如，追踪加密货币交易，对于追踪者来说。在暗网和区块链上使用开源调查只是前奏。您能做到的就是，尽可能清晰地呈现目标交易网络节点之间的关系。

至于那些节点的真实身份，将取决于相关方以及加密货币交易所自己的内部管理，以查找与暗网上的特定活动相关的任何帐户的注册详细信息。

显然，这些信息只有政府才能拿到。

这不是个公平的游戏。如果您的调查目标是诈骗犯、儿童色情创作者、毒贩、非法军火商 …… 警察和政府间谍很可能愿意帮你；但是，如果您在挖掘政府官员的非法资金来源、信息战的雇用关系、操纵选举的黑钱等等 …… 您知道难度在哪里。

这就是为什么我们在2018年访谈中强调开源情报是 “退一步” 的想法，而不是进一步，透明度革命从来都是最重要的 —— 我们需要知情人说真话。 BACK https://medium.com/@iyouport/%E6%83%85%E6%8A%A5%E4%B8%8D%E6%98%AF%E7%AE%80%E5%8D%95%E7%9A%84%E4%BF%A1%E6%81%AF-iyouport-%E7%AD%94%E8%AF%BB%E8%80%85%E9%97%AE-%E5%85%B3%E4%BA%8E%E6%88%91%E4%BB%AC%E4%B8%BA%E4%BB%80%E4%B9%88%E8%80%8C%E5%AD%98%E5%9C%A8-%E4%B8%8B-b1f127d81cb2

3、与隐私倡导相悖

这是很显然的。开源情报之所以能成功，是因为有太多的人不注重隐私保护。当我们的数字权利倡导取得成功的时候，将以开源情报难度加大为标志。

而这才是我们真正应该期待的。

开源情报追踪针对那些毫无戒心的普通互联网用户尤其有效，然而真正做坏事的人，往往都具备较为强大的隐私意识，他们很注重反情报防御。

于是，你知道，政府用它来追踪活动家和异议人士的效率比追踪毒贩和恐怖分子要高得多。后者甚至可以将自己的行为栽赃给无辜者，就如网络攻击中的惯用手段“假旗 FlaseFlag”。

这绝不是高抬毒贩，而是说，如今活动家必须能有毒贩那种水准的防御意识，才有可能躲避当权者的围捕。 [image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

[image]

我们对开源情报的使用

开源情报演示和思考方式应该被普及，因为这是理所应当的均权。互联网上的一切（除了付费内容外）对所有人来说都应该是公平的，每个人都应该随时可以找到自己想要的知识。

没有人应该被囚禁在回音壁气泡里、或者被 Twitter 和 Facebook 的算法所控制，也没有人应该被虚假消息所愚弄，但前提是，更多人了解科学的互联网用法。这是开源情报演示和思考方式讲解能带给大众的另一份利好。

我们在去年底的《新10年》中发布过这一邀请，请读者使用我们提供的工具和技巧与周边的朋友对话—— 比如 “这个消息是真的吗？”、“这个图片被PS过吗？”、“我的设备出现了奇怪的反应，我被黑了吗？”、“那个象形字是什么意思” …… 等等。这将锻炼您快速准确的信息检索、信息验证、以及对安防技巧的运用。

您可以为身边的朋友展示 “为什么这条消息是假的”，是通过哪种方法/哪条路径找到的证据；如何验证一张图像或一个视频被操纵了 …… 想要采访对象的私人电子邮件和电话号码吗，通过 LinkedIn、Facebook、抖音、Twitter 等平台也许就可以找到，如果目标人使用这些平台的话。

您甚至可以尝试做一些游戏，比如以微信朋友圈用户上传的照片为案例，请大家一起来判断 “你能从这张照片中读出哪些隐藏的信息？—— 追踪线索”。

这些游戏会很吸引人，尤其是，所有参与者和围观者都能通过观察和思考发现在安全保护方面自己应该做些什么。

就连平日对技术不感兴趣的人也会加入进来，因为人们看到它可以不需要编程基础、一点都不难。而且很好玩。

还可以更激进一些，邀请人们对自己使用这些追踪技术，以检查自己在数字世界里暴露了什么，尤其是，如何快速切断隐患。 BACK

[image] 自我人肉

借此同时再次介绍全面的自我保护技术，从化名到分身，从在线到现实，切断追踪线索的方法，您将发现，会有更多人对此感兴趣。

最后

本文是希望您对开源情报有一个比较客观的了解，关于它能做什么、不能做什么、以及最好用来做什么的认识。

我们始终认为，不论是开源情报还是透明度革命，不论是传统抗议还是黑客行动主义，它们都无法单独完成变革的目标 ：

- 透明度革命中对吹哨人提供的资料需要开源情报技术以验证真伪；
- 开源情报追踪调查需要透明度革命的支持才能挖掘到更深层内幕；
- 传统抗议需要开源情报思考方式以躲避监控镇压；
- 黑客主义行动计划既需要开源情报做侦查手段也需要透明度革命带来的曝光作为知情基础，还需要社交工程战术以获得入口 ……
- 我们希望介绍它们所有，因为它们的确是一套综合性的知识 ，关于，如果想要成功您需要什么。

您可以将这些知识进行最适当的组合以满足您的具体目标。期待您的伟大成就。

[image]
[image]

在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作

[image] 关键词	反追踪 生物识别 社交媒体
[image] 关联	[image]匿名着装 ；[image]生物特征隐藏 ；🔍开源情报
[image] 创建时间	2020年10月14日
[image] **Description**	操作安全性；行动安全性

作为参与者，您应该有意识地保护行动整体的安全，当然包括您的个人安全。

- Table of Contents

步骤1：删除地理标签和其他元数据
选项1：从照片中删除地理标记和其他元数据
选项2：从视频中删除地理标记和其他元数据
步骤2：隐藏和模糊化面部及任何可识别性信息线索
选项1：遮盖照片中的信息
选项2：遮盖视频中的信息
步骤3：使用匿名帐户发布
步骤4：在线发布照片之前使用VPN
最后

[image]

从去年十几个国家/地区参与的抗议活动开始（包括香港），直到今年BLM带动的多个国家联合的抗议运动，各种群体反抗一直在激增，示威游行的有力照片和录像吸引了全世界的目光。

如果在线上传照片之前没有采取保护措施，那么这些照片可能会使您或其他人处于危险之中。

[image]

返回：[image]当您准备参加抗议活动：基本指南

返回：[image]您需要真正的“自己人”：整体安全S01E09 - 进入战斗状态

返回：行动安全性总述

在抗议活动中拍摄和记录证据非常重要。这不仅可以避免被警察反咬，而且有些时候还能发现警方的渗透者。

尤其是，媒体捕捉的镜头经常很片面，甚至有误导性 —— 企业媒体甚至会埋没真正的抗议目的。

但不论是抗议者的脸部出现在新闻报道中，还是被警方的社交媒体情报所捕获，都很可能导致被捕、被骚扰甚至更糟。

因此，采取预防性隐私措施至关重要。

如果您参加了抗议活动并想要分享图像，您需要知道，保护自己的身份以及您拍摄到的其他人的身份至关重要。

本文将讨论的是在社交媒体上发布抗议图片和视频之前应采取的步骤，例如 剥离元数据，模糊面孔和任何可识别性信息线索，使用匿名帐户或一次性帐户等等。

步骤1：删除地理标签和其他元数据

Exif 数据是数码相机（包括智能手机相机）记录的元数据。

数据为摄影师提供了有关所用相机设置的有用信息，例如光圈、ISO 感光度、焦距、闪光灯使用、曝光时间、变焦级别、分辨率、色彩空间等。

尽管这些功能很有用，但其中包含的数据也可以用来跟踪您和您拍摄的照片的位置，包括黑客和警察，几乎任何人都可以使用该信息来了解您去过的地方和您的身份。

最敏感的信息是地理标签或地理坐标，它们可以精确地指出拍摄图像或视频的确切位置。

然后是所用相机的制造商和型号、其软件以及时间和日期，所有这些都可以定位您。甚至还有加速度和高度数据，后者可以说出您是在地面上还是在几层楼上拍摄的该图像或视频。

对于智能手机，有很多选项可以从照片和视频中删除GPS数据和其他元数据。不过并非所有功能或应用程序都适用于所有类型的视觉媒体，甚至不能在所有移动操作系统上通用。

尽管某些社交媒体网站（包括 Facebook、Twitter 和 Instagram）会自动隐藏元数据，但那只是对其他用户不可见而已，平台自己会保留，随时可能交给警察。于是您最好是在上传之前手动安全地删除元数据。

选项1：从照片中删除地理标记和其他元数据

[image]

从本站“工具”专题中搜索“元数据”，已找到相应工具。

如上所述，有许多不同的方法可以从照片中删除地理标记和其他元数据。在进入删除大多数 Exif 数据的第三方应用程序之前，您的设备中

可能就有从图像中删除位置数据的本地功能。您需要使用它。

在iOS上，您可以先删除任何照片的位置数据，然后再从 “照片” 应用中共享它。在 Android 上也许复杂一些，具体取决于您的设备的品牌和型号。

例如，在 Samsung Galaxy 的 Gallery 应用程序中，您可以向上滑动图像以显示其详细信息，点击 “编辑”，然后删除位置。

如果您主要将 Google 相册用作保存视频和照片的地方，例如在 Pixel 手机上，除非您的设备 “估计” 了该位置，否则您无法删除该位置（在照片上滑动，点击该位置旁边的“ 更多信息”，然后点击 “没有位置”），但是在通过Google 相册共享图像时，您可以禁用位置共享。

[image] [image]

另外，您可以简单地在 iPhone 或 Android 上拍摄任何照片的屏幕快照，这不仅能自动从原始图像中删除位置标签，而且还会删除所有其他Exif元数据。

但是，这样做会降低照片的质量。如果您急于想要在线上传照片，这是一个可行的选择，但是对于其他所有功能，还有第三方应用程序可以做得更好。

对于 iOS,，例如 Exif Metadata, Metapho, HashPhotos, Exif Viewer, Koredoko, ViewExif, 和 Photo & Video Metadata Remover，都可以从图片中清除地理标记和其他元数据。

其中很多应用还允许您编辑元数据，因此您可以通过更改拍摄图像的实际位置来愚弄监视者。当然，你知道，假消息制作者也会这么干。

另一方面，在 Android 上，有诸如 ExifTool, Scrambled Exif, 和 Photo Stripper 之类的应用程序，可以擦除所有Exif信息。

您可以使用的最佳选择之一是跨平台的开源工具，因此您可以在拥有

的任何设备（包括计算机）上使用它。它被称为 Image Scrubber，它可以在任何Web浏览器上正常运行。

上传图像后，它会向您显示其所有 Exif 数据，然后可以在其中 “清理” 它。如果要从视频中捕获静止图像，也可以上传视频并选择帧，然后查看和清理 Exif 详细信息（如果有的话）。

[image] [image]

选项2：从视频中删除地理标记和其他元数据

视频的发布与静态图片一样多，甚至更多，您也可以从其中剥离元数据。但是，对于智能手机上的本机 Exif 删除工具来说，可能没有太多选择。

如上所述，您可以通过 “照片” 应用程序使用iOS 13的删除选项，前文中概述的有关从 Google 相册中删除照片位置数据的方法也适用于视频，但是三星禁止从视频中删除 Exif。

当涉及到第三方工具时，适合处理图像的许多应用程序也都可用于视频。以下将简要展示适用于iOS的照片和视频元数据删除器以及适用于 Android 的 ExifTool，它们都是免费工具。

- 使用照片和视频元数据删除器（**iOS**）

打开 “Photo & Video Metadata Remover” 应用，从 “照片” 应用中选择一个视频，点击出现在视频左下方的齿轮图标，然后选择 “清除所有元数据”。不含任何元数据的新视频将保存到您的设备中。

[image] [image]

- 使用 **ExifTool**（**Android**）

打开 ExifTool 应用程序，从图库中选择一个视频，您将看到该视频的元数据分成不同的组。

点击右下角的三条线菜单按钮，选择“全部擦除”，然后选择“是”进行确认。它将删除所有可删除的元数据，例如位置和日期等，但保留其他无用的元数据。

[image] [image] [image]

步骤2：隐藏和模糊化面部及任何可识别性信息线索

除了剥离元数据外，保护照片和视频中的人物脸部及疤痕等、以及地理位置标记（例如路牌等）也至关重要。

[image]

可以很容易地从照片或视频中识别出面孔、标志性衣着、疤痕、纹身、胎记、地址、企业挂牌、广告牌、和著名地标等线索。也就是您在 “开源情报” 地理定位操作中第一步要瞄准的那些东西。

甚至独特的衬衫设计也可以帮助识别一个人。

尽可能隐藏面部和可识别性信息的最佳方法是将其模糊或涂黑。模糊效果很好，总体上看效果最好，涂黑会更安全，因为无法逆转效果。

但只要您使用在智能手机上处理模糊化效果的工具、并且不要将副本保存在所谓的云中，对大多数人来说这就足够了。

选项1：遮盖照片中的信息

如果您只想涂黑（或使用其他纯色），那么智能手机上的本机工具就足以完成任务。

对于 iPhone，在“照片”应用中查看图像时，点击 “编辑”，然后点击省略号（•••），然后点击 “标记”。在这里您可以使用纯墨水和钢笔、铅笔或形状的工具来隐藏对象。

对于三星 Galaxy 手机，在 “Gallery” 应用中打开图像，点击工具栏中的笔图标，然后点击绘画图标。点击出现的钢笔图标以选择笔尖和强度。您还可以使用贴纸工具将有趣的贴纸放在敏感信息上。

如果使用 Google 相册，请点击工具栏中的波浪线图标。选择标记工具，黑色墨水（或另一种颜色），然后随便画就行了。

[image] [image]

但是没有本机模糊工具，因此如果您想要模糊化处理，则需要使用第三方工具。

Signal 刚推出了用于其安全消息传递应用程序的模糊工具，并提供了自动和手动选项以遮盖面孔，您可以在编辑图像后下载图像，而无需在其中共享消息。

除此之外，还有许多其他可用的工具，您可以在应用商店中进行搜索，但是最简单的工具之一是 Image Scrubber，上面已经讨论过了。

这是一个跨平台的网络应用程序，还可以使您模糊或涂黑照片中的某些部分。开发人员 Pipkin 声明，Image Scrubber 不会在任何地方共享您的信息，并且所有图像处理都在您的设备上的Web浏览器中进行（源代码在这里）。

[image] [image]

选项2：遮盖视频中的信息

尽管视频比照片更难更改，但模糊任何面部、地址、车牌号和其他可识别性信息仍然很重要。

您可以使用许多第三方应用程序做到这点，但是有两个免费且不包含水印的流行应用程序分别是 iOS 的 Video Mosaic App 和 Android 的 Blur Video。

- **Photo & Video Mosaic App（iOS）**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊的画面从开始和结束的确切位置。

在这里您可以使用各种功能向面部、地址、文本、车牌、建筑物等添加模糊效果。使用该应用底部的工具更改模糊强度和效果。完成后，将编辑后的视频保存回本地 “照片” 应用程序。

[image] [image]

- **Blur Video (Android)**

在 Video Mosaic 中打开一个视频。使用视频下方的预览栏，您可以滚动到要模糊部分的开始和结束的确切位置。过程如上所述一样，完成后，将编辑后的视频保存回本地 “照片” 应用程序。

[image] [image]

步骤3：使用匿名帐户发布

如上述这些方法，删除元数据并模糊一切可识别性信息可以保护其他人，但是，如果您将照片和视频发布在个人帐户上，那么追踪您就易如反掌了。

只要监视者在您的帐户上找到抗议照片，就可以通过查看 “朋友列表”、阅读旧帖子、访问您的其他在线帐户的链接等等形式，了解您生活的几乎全部。

这就是为什么最好的选择是发布到匿名帐户或个人信息相对较少的帐户。在下面看到具体方法：

[image]

返回：[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

如果您要在网上发布抗议现场照片，Twitter 是最好的选择，仅仅是因为保持匿名和获得关注度更容易。

在 Instagram 上就有点困难了。但只要未与个人帐户建立任何联系，您就可以创建并发布 Finsta —— 即 fake Instagram。

[image] [image]

您还可以使用匿名 Facebook 帐户发布抗议照片。在下面看到具体指南，关于如何设置虚假的 Facebook 个人资料、如何创建一次性电子邮件或电话号码，将应用程序与手机数据隔离，使用VPN，删除和禁用位置记录，更改隐私设置等等。

此外，即使您使用匿名帐户发布信息，也请务必从您的信息中删除您的位置。

尽管您可以在发布时删除坐标，但您可能会无意中将其地理位置信息添加到了帖子中。在大多数情况下很容易避免这点。在 Instagram 和 Facebook 上，您所需要做的就是不手动包含您的位置。

但是，在 Twitter 上，可能会跟踪您的精确坐标。

要关闭位置数据，点击左上方的个人资料照片，依次转到 “设置和隐私”，然后转到 “隐私和安全”。向下滚动并点击 “精确位置” 并将其禁用。

[image] [image]

步骤4：在线发布照片之前使用VPN

这应该就不必细说了。至少中国用户使用 Twitter 或 Facebook 时必需加VPN。

但是，如果您不在中国，可能就很容易忘记**VPN**的使用，不要。尤其

是选择可靠的VPN，您需要熟记方法（而不是去问其他人“这个或那个可靠吗”），您应该自己判断 —— 您可能无法知道他们中哪位是拿钱说话的人。

[image]

返回：[image]如何检查您的VPN连接是否实际加密

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

最后

在本站专题 ❤🔥行动安全性-OPSEC 中读到更多具体内容。

参加抗议活动是一种“特殊时刻”，即便您自己不担心被捕，您也应该希望您参加的活动能真正发挥作用，至少不那么容易被迅速扼杀掉。所以，每一位参与者都应该努力维护运动的目标，首先就是信息安全。

希望您的所有队友都具备足够的安全意识。

[image]
[image]

给活动家的反人肉指南

[image] 关键词	人肉 反侦察 反追踪 对抗性思考方式 自卫 预防性
[image] 关联	[image]如何知道有人正在线人肉你？6个简单的方法
[image] 创建时间	2021年3月24日
[image] **Description**	操作安全性

人肉狂的目的就是让你绝望而放弃自己的反抗事业，这是所有形式的镇压的宗旨。而您的宗旨就是，别让他们得逞。

- Table of Contents

什么是**Doxxing**
一分预防胜过十分治疗
少即是多
亲属 ——
政治 ——
朋友与社区 ——
兴趣爱好 ——
法定信息 ——
事业 ——
策略
从自我人肉开始
更改用户名，电子邮件地址和密码
整理可用内容并更改您的隐私设置
如果您已经被人肉
注意事项
评估威胁
问自己以下这些问题：
解决方案
与同事和家人进行对话

不要妥协，继续前进
以下是您可能选择采用的一些措施：

[image]

这里的分步指南将解释如何保护自己免受网络人肉的侵害，为什么这很重要，以及如果你已经成为了人肉迫害的目标，该怎么办。

在一个普遍监控的时代，当社交网络用户转播每一次重大的示威活动时，恶意的个人、政府间谍和警察都会密切梳理社交媒体的帖子，收集情报以骚扰活动家，因此，您必须做好应对的准备。 https://iyouport.substack.com/p/blm6?utm_source=publication-search

什么是Doxxing

这里所指的 Doxxing 是专门针对异议人士和反抗者的一种可能非常可怕的镇压手段，它通过公布一个人的私人信息，目的是曝光和恐吓此人放弃反抗。这可能对目标造成身体、情感和经济等各方面的伤害。它的目的是吓倒反抗者让他们放弃行动，并使他们的想法和价值观受到羞辱。

重要的是，在你被 Doxxing 之前，要认真对待安全问题 —— 在你甚至有理由担心自己可能被 **Doxxing** 之前进入防御，而不是亡羊补牢。

通常，Doxxing 会等到收集到了足够多的信息后才一次性爆炸；那时候您有可能已经被跟踪很久了，直到为时已晚才发现。

无论您是知名的公开身份的活动家还是几乎没有参与过任何行动，您都应该保护自己的社交网络和生活中的其他领域 —— 即使您不认为自己正在做任何值得关注的事，也是如此；要知道，这些坏蛋是完全没有原则的。

保持良好的做法可以保护您自己、您的朋友、家人和社区。Doxxing 只需要一条信息就可以开始在网上寻求更多的细节，他们会挖得很深，他们都是🔍开源情报 界最邪恶的疯子。

[image]

您必须意识到自己在网上留下的任何信息痕迹，都有可能令您受到警察、间谍、以及莫名其妙的疯子的侵害。现在，国家实施的监控越来越复杂，同时在抗议活动中进行在线直播已经成为常态，仅仅戴上面具往往是不够的。

2020年6月，在费城，调查人员从一个女人的模糊照片开始确认她的身份。他们跟踪了一整条数字面包屑的线索，包括网购、Twitter 账户、和她的专业工作页面 ……你永远都不会知道他们会将什么做成武器以击倒你。

任何时候，请确保您的在线存在可以让您感觉在线下采取行动更安全。

[image]

一分预防胜过十分治疗

没有比现在更好的时机了，您应该马上开始。因为，如果您已经被 dox，您就很可能无法再删除那些坏蛋用来打倒您的被武器化的您的个人信息，因为它们会被无限地复制粘贴，您永远都删不掉。

有许多不同的方法来解决这个问题。显然，确保没有人可以找到任何关于您的信息的最好方法是 —— 没有任何可用的信息在线，但有些人无法消除自己的在线存在，无论是因为工作、家庭、或者其他责任。

在某些情况下，保持某种在线角色是有战略性原因的；例如，拥有一个长期存在的、可信的但完全无害的社交媒体账户，可能对应付查手机来说非常有用，比如当您跨越美国边境的时候，或者当您进入新疆

地区的时候。

也就是说，您可以采取分身战术，将自己敏感的部分隔离出来 BACK 分身 。

有一些方法可以将您生活中不同的领域设置成防火墙，如果您需要的话，可以策划一个公共档案，并采取一些做法，帮助您和您的朋友感到有能力继续在您的社区中采取行动。

这个过程可能是乏味的。它将需要时间和精力。建议您与朋友，室友或家庭成员一起做，以帮助度过一些困难或无聊的方面。

少即是多

如果您不能完全从互联网上删除自己，您仍然可以通过保持不同的领域的在线活动来保持相对的隐私，并清理那些被遗忘的或不经常使用的账户。

您很可能有一个以上的在线存在。这可能包括社交网络、留言板、工作网站、电子邮件账户等等 —— 任何您需要登录的东西。通常在 doxxing 中，信息是从许多不同的来源进行三角测量的。减少信息量的方法之一就是，分割这些领域，使它们彼此不连接，将人肉狂带入死胡同。

这是一个高度个性化的过程；花一些时间考虑以下问题，以绘制出最适合您自己的做法：

- 您是否把时间花在社交媒体熟人间的讨论上了？
- 您是否经常点赞或转发激进的社交媒体帖子？
- 您在任何招聘网站上有个人信息吗？

- 您是否在任何网购站点上买东西？

- 您的朋友在社交媒体上发布过您的照片吗？

- 您是否需要在网上宣传自己所从事的工作？

- 您是否用同一个账号与您的同事、家人和活动家朋友联系？

- 您是否使用部分真实姓名或真实生日作为用户名或电子邮件？

每一种情况本身可能都不是问题，但是，当它们被放在一起时，就是您的完整私密生活图谱，警察和间谍等人肉狂最想要的就是这个。他们会这样做，比如：https://web.archive.org/web/20201004211840/https://www.iyouport.org/%E4%BB%8E%E8%B7%A8%E5%B9%B3%E5%8F%B0%E8%B7%9F%E8%B8%AA%E5%88%B0%E5%BF%83%E7%90%86%E5%88%86%E6%9E%90%EF%BC%9A%E7%A4%BE%E4%BA%A4%E5%AA%92%E4%BD%93%E6%83%85%E6%8A%A5%E6%94%B6%E9%9B%86%E7%AE%80%E6%98%93/

您需要问自己以下这些问题：

- 这些账户/身份的独立性如何？—— 会不会像上图中那样，只要找到其中一个账户/身份，就能牵出一大串其他东西？

- 哪些是公开的？哪些是私密的？—— 您肯定知道什么时候应该公开，什么时候应该私密；

- 在每个网站的背景中，公共和私密意味着什么？—— 这是对开源*反*情报而言的，您必须从技术角度来考虑这件事，而不是简单地信任某平台上的隐私设置按钮；

- 通过搜索您的法定名称可以在网上找到什么？—— 这是指您需要 [image]自我人肉 一下，以便了解自己真正的曝光程度，而不是靠想当然；

- 您是否在多个账户中使用同一个用户名或电子邮件名？这些是否在您的生活中交叉到不同的领域？—— 花点时间想想所有这些领域在线下重叠的方式；

- 您的工作是否允许您公开自己的政治倾向？—— 有些时候是不允许的，比如存在政治审查的工作，您的雇会因您的政治倾向而解雇您， https://iyouport.substack.com/p/26d?utm_source=publication-search ；

- 您的行动主义有多公开？您会和记者交流吗？您在宣传自己吗？—— 这需要权衡，建议您使用这里的标准来科学地权衡这点 [image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

- 您是否会过滤部分或全部来自亲属的社交媒体内容？—— 很多人会这样做，有些时候这有必要，但是，这也会导致您无法及时看到您的亲属是否发布了曝光您真实身份的信息，您应该在发现这种情况后立即要求对方删除，所以，及时获知是很重要的。警察和间谍很擅长利用您的身边人来对付您，而不是直接瞄准您本人；

- 在您的特定个人资料中是否有任何提及非法的或有争议的活动？不论那是不是真的发生过 —— 这些信息不论真假，都是追踪狂的挚爱，他们会无限放大这些信息，借以对您实施人格暗杀。

[image]

以下是一些示例，说明您的在线形象如何在不同站点上重叠：

亲属 ——

您与您的亲人之间的关系有多公开？尽可能把所有亲人考虑进去，父亲、祖父母、兄弟姐妹、七八姑八大姨 …… 思考这个问题：如果恶意者获得了他们中任何一个人的信息，恶意者可以从中挖掘到关于您的多少内容？

政治 ——

您是否曾经在网上讨论或发布过有关您的政治立场的信息？如果是，在哪些平台上发布的？

朋友与社区 ——

如果您有社交媒体，您的朋友是谁？您的追随者是谁？您的在线社区是否或以何种方式反映了您的现实生活？

兴趣爱好 ——

您有什么爱好？您有基于兴趣爱好结交的朋友和参加的相关社区吗？您是致力于这些爱好的互联网社区的一员吗？

法定信息 ——

您的真实身份绑定了哪些电话号码和地址？您的帐户中是否包含法定身份信息？还有其他网站包含您的法定身份信息吗（包括可能未经您的许可的情况下被收集的信息）？比如您通过手机号码验证了一项服务，该服务就有您所有法定身份信息。

事业 ——

您的工作是否涉及在线业务、网站或社交媒体帐户？如果您的政治立场与您的职业重叠，会不会有问题？或者，您的职业生涯在某种程度

上与您的政治身份有关？

花时间考虑一下您的真实身份与在线身份的重叠之处，在线目标是什么、以及可以将这些领域分开的方法。

[image]

策略

下面来看看如何发现您的哪些信息、如何识别和消除这些痕迹，以及有哪些在线资源可以删除它们。

从公开的信息开始。谷歌您自己，列出您所有的社交媒体账户。删除您不再使用的旧账户。这也是一个很好的时机，下载一个密码管理器，如 1Password 或 LastPass，协助您管理独特的用户名、电子邮件和密码。

从自我人肉开始

就如您所知道的，要想做到最有效的防御，您需要想攻击者那样思考。想想看人肉狂会怎么做？没错，他们会先彻底挖掘有关您的一切，所以防御的第一步就是，抢在攻击者行动之前您来亲手挖掘自己的一切，把能删除的所有部分都删掉。 [image]自我人肉

并不是所有东西都能删除，有些是删不掉的，比如曾经的联署信，如果您使用了自己的真实身份的话。总之，把您能删掉的一切都删除，并制作一些假的身份信息，以迷惑人肉狂。

并且，您还可以设置提醒，如果有人在搜索您，您会收到警报， [image]如何知道有人正在线人肉你？6个简单的方法 。

在这个初步的搜索之后，再看看那些靠买卖个人数据获利的数据中介网站。这些网站会尽量让你难以删除自己的信息。耐心一些，因为人肉狂会非常耐心地挖到您的一切。 [image]单向镜的背后：监视资

本家和政府的联手一直在如何折腾你？

当您在网上搜索自己的时候，您也可能会发现旧的账号，使用您能记住的所有旧用户名和网名进行反向搜索以找到它们，我敢保证肯定有您早已忘掉的自己注册的账户。

您很久没有使用过的账户会让您变得脆弱，因为如果他们使用的是旧的密码，人肉狂可以尝试将密码用于其他账户。下载任何对您有感情价值的资料，永久关闭所有您不再使用的账户。这里面可能充满了关于您生活的线索。

这是您要是使用开源情报的地方，因为人肉狂都是开源情报专家，您需要像他们一样专，才有可能战胜他们。

Haveibeenpwned.com 将帮助您确定是否有涉及您所拥有帐户的数据泄露。如果有，请立即采取措施更改密码。

[image]

更改用户名，电子邮件地址和密码

别人要想找到更多关于您的信息，最简单的方法就是搜索您的名字、别名和用户名。为了保持您的互联网活动范围分开，每当您创建一个帐户时，总是需要使用一个新的用户名，一个完全不一样的用户名，没人能将它们和您联系在一起的那种。

如果您有一个专业的工作网站，必须使用您的法定名称，请确保您用于该账户的电子邮件只用于该目的 —— 所有医疗和政府相关的账户有一个名字，网购有一个名字，政治生活有另一个，社交媒体也有另一个，交友网站再有另一个 ……对所有代表您或展示您照片的网站都使用别名和虚假身份信息。

整理可用内容并更改您的隐私设置

一旦您消除了所有的枝节，就可以开始选择要保留的东西了，以及在那里可以找到什么。如果您保留了任何社交媒体账户，请先翻阅您的个人资料，并思考其他人可以从中发现关于您的什么。

一些选择包括：

- 删除所有自己的照片，您的宠物，您的车，您的邮箱，纹身，和其他任何东西，包括不必要的识别性信息，特别是您的公共档案图片。

- 删除或伪造个人资料中的任何个人信息 —— 提供一个假的生日，随意编写任何关于家乡、上过的学校、雇主等等信息。

- 如果您把所有的社交媒体设置都改为私密，并且对自己的关注者名单有信心，那么可能就没有那么多理由隐藏您的脸。但是仍然要建议将有关您的位置和私密的个人生活的细节保持在线下。如果您选择更加公开，请将您的朋友和家人分开，在没有得到他们的知情同意的情况下，不要发布任何他们的照片或他们的个人信息，并记住，通过社交网络和数据收集网站可以很容易看到社交关系，人肉狂总是会从您的周边人下手。

当您认为自己已经完成了，试着让一个朋友根据他们能找到的关于你的信息创建一个配置文件，看看是否有任何您没有想到的东西被漏掉了，快速找到解决方法。每隔几个月定期检查一下通过搜索您的名字能找到什么，这可能很重要。

如果您已经被人肉

如果已经发生这种情况，永远不建议报警。警察会使用他们得到的关于您和其他个人和团体的信息，您可能已经公开的那些关系。一旦这些信息被记录在案，就会永久地掌握在警察手中，这个您是删不掉的，而且警察很可能用这些信息来针对你或你的队友进行镇压。

通常情况下，警察不会做任何事，或者只会使情况变得更糟。本指南的目的是为您提供基于社区支持和授权的替代方案。

您需要公开回应，但在此之前请务先与您的关系网络沟通这件事。

您的第一反应可能是立即用公告这件事以提醒尽可能多的人，或者关闭一切。如果您有支持者群体，以这种方式公开可以为你提供即时的支持，但是，这样做也有可能增加人肉狂的攻击性。

[image]

您首先要做的最重要的事是 —— 采取措施保护自己和您的关系网络，免受进一步的伤害。

而立即发布公告会使您的安全工作变得复杂。无论被人肉狂发布的关于您的信息是否准确，在没有首先确认至少部分信息的情况下，没有人可能利用这些信息对您造成任何严重的伤害。

立刻公开还会表明您已经看到了攻击发生，并表明您很害怕。人肉狂想要的就是这样的效果。他们想恐吓和孤立您。

[image]

不要确认或否认他们挖到的任何关于您的信息，不管它是假的还是令人尴尬的。人肉狂正在寻求您的这种反应。如果您让他们知道他们所发布的信息是不正确的，他们可能会得出结论，他们是在正确的轨道上，他们只需要继续挖掘。

有时，最有效的初始公开回应之一就是完全不回应 —— 不要对您的发帖习惯做出任何重大改变，也不要表现出任何恐惧。这可以传递这样的信息：doxxing 目标是错误的，你们的攻击是失败的。

在您有时间处理自己的感受并确保自己的安全之后，再公开发表意见，或许可以和其他遭遇类似情况的人联合起来，这可能是一种战略性的做法。

您也许可以利用公众对攻击者的愤怒来创建一个运动，以劝阻进一步的迫害 —— 例如，做一个资助活动，承诺为您和您的社区中的其他遭到骚扰的人分钱，由于骚扰者想要孤立你，这样的公众支持可以阻止进一步的恐吓。

[image]

尽量做到有创意、有弹性、有策略。在这个过程中，要小心不要危及到其他任何人。

在发表公开声明时，如果您摆出姿态或吹嘘自己的能力、尤其是使用暴力的能力、可以保护自己的武器，或者过分夸大自己的凶残等等，绝不是好事！这只会伤害您的支持者，却很难吓到攻击者。

建议您发表积极的声明，申明您的道德和信仰，描述您的身份或您的理想如何使您成为被攻击的目标，并且一定要坚强，强调虽然这些骚扰活动是为了让你退缩，但你不会这样做，因为你没有理由隐藏自己的政治立场。请避免谈论任何具体的行动或团体，无论你是否参与其中。

[image]

注意事项

1、不要惊慌地打电话给朋友过来帮忙。

2、建立一个事件日志，并对在线和离线的挑衅行为进行记录。这对于确定攻击模式至关重要！将您的记录与您的伙伴中同样遭遇者的记录进行对比，您有可能从中看出更大范围的攻击模式，从而确定您的对手和他们的组织，这是很有用的。

3、私下里提醒您的朋友、家人和敏感的政治网络。责成几个您信任的朋友提供您的个人信息，帮助报告社交媒体和博客帖子，确定它们是骚扰。反复这样做。

有时人肉狂会使用您的照片和个人身份信息来冒充您的账户。通常，将这些作为假货进行举报比较容易；为了防止他们通过冒充您的身份从您的敏感关系网络中获取更多的信息，请尽量尽快举报。

您自己、您的家人和您的雇主可能会开始收到威胁或骚扰电话。尽快让他们知道发生了什么，并指示他们不要与骚扰者接触。

4、关闭信息流。如果您还没有进行预防护理部分，请马上开始这个过程。下载一个密码管理器，立即更改您的所有密码。

重要的是要尽可能减少信息曝光导致的“出血”，同时也不要让人肉狂警觉到dox是有效的或有针对性的。尽量通过将好友列表和信息私密化来支撑您的社交媒体账户，以保护您的关系网络中的其他人，直到您确定他们不会将脆弱的个人信息提供给那些愿意挖掘的人。

您如何公开反应是一个非常微妙的情况，在整个过程中应该小心处理。

5、制定一个安全计划。招募朋友和家人来支持您。让他们知道正在发生的一切；doxxing可能是创伤性的，您需要优先考虑自己的心理和身体健康，以便继续您的工作。

这些对话可能会很困难 —— 特别是如果您的亲友不了解这个政治时刻的细微之处，如果他们是第一次听到有关这种镇压方式，或者如果您和亲友之间的关系因政治立场或个人差异而紧张。如果您觉得自己无法胜任，可以请一位对情况很了解的朋友替您进行这种困难的对话。

如果您的家庭地址成为了人肉目标，如果可以的话，找一个新的藏身之处。如果您不能离开家，邀请朋友或当地的安全团体与您同住。做一个“随身包”，里面装上您需要的所有东西，以便您随时可以立刻离开此地。 [image] S04完美隐身-总章节：机智是重要实力

评估威胁

如果您不觉得自己有非常大的风险，特别是如果针对您进行攻击的人肉行动是由免费提供的信息组成的，或者是直接发给您的，目的是为了激怒您，您可能会觉得无所谓，把它当做一种廉价的恐吓策略，屏蔽并报告骚扰者，然后继续前进。

但如果针对您的人肉包括敏感的个人信息，特别是不容易通过简单的侦查工作就能获得的细节性信息，您可能要采取进一步的预防措施。如果您已经是被攻击的目标群体或社区的一部分，尤其如此。

当您了解到自己已经被 dox 时，重要的是要确定哪些信息可以转化为可信的威胁。通常情况下，doxxing 是更具侵入性的线下骚扰的前兆，或者与对信息采取行动的威胁有关。这可能是任何事，比如报假警、给您的家人亲友或工作单位打骚扰电话、死亡威胁等等。

有时很难确定什么使威胁 “可信”。普通人肉狂最常见的策略是在他们认为能联系到你的任何地方发送令人毛骨悚然的或恐吓性的信息 ——社交媒体、电子邮件、家庭成员等。攻击者经常会暗示他们拥有比实际更多的信息；他们通常会说他们已经向当地执法部门提供了这些信息。他们的目标是恐吓你不要采取行动；您需要知道，通常他们公开发布的任何关于您的信息都是他们获得的全部信息。

你的雇主可能会接到电话，人肉狂要求他们解雇你。到目前为止，被人肉的目标很少受到人身攻击，但它确实已经发生了，那些人肉狂可能会努力将你的信息送到那些不道德的人手中，激励那些疯子去殴打您。

谨慎是重要的，但不要惊慌失措，也不要沉浸在焦虑中。

问自己以下这些问题：

- 用来人肉您的信息是否准确？人肉狂有你的家庭、工作单位或

家庭地址吗？他们知道你常去的地方吗？他们知道你的朋友是谁？

- 如果他们发现了你的这些信息，你是否有失业的风险？

- 你知道骚扰者住在哪里吗？他们是靠近你的实体社区，还是只是分散在论坛上的在线trolls？

- 他们是否有你的敏感照片（尴尬的和私密的照片）？

- 他们是否有信息将你与犯罪活动联系在一起，可能会让你被捕？比如污蔑您持有毒品？或者污蔑您的私生活？

[image]

解决方案

您可以采取以下措施来应对人肉的危险：

- 制定自卫计划，参加自卫课程，联系当地社区防卫组织；具体方法见《灾难中幸存》系列，此处为本系列最后一集，含完全列表；

- 通知被点名的人和团体 —— 工作单位、同志、室友、家人，让他们做好防御；

- 和您信任的人谈谈您的恐惧；

- 联系曾经经历过这种情况的人，征求他们的意见；

- 如果您担心有关您的信息可能会引起国家行为者的兴趣（警察和政府间谍），请安排一名律师；

- 与当地的反抗组织联系 —— 如果人肉狂是用假账户发帖，他们也许能帮助识别人肉狂的身份。即 反向人肉。

与同事和家人进行对话

这种对话可能会非常困难，尤其是当您的家人不支持您的事业而造成你们之间关系紧张时。如果有必要的话，让一个头脑冷静的朋友在事后帮助调解或支持你。

想一想，您愿意多长时间和家人脆弱地交谈一次，将来又有多少机会跟进这次谈话。如果有必要和家人交谈，但您觉得自己只有一次机会，可以和朋友排练一下，为您将面临的反应做好准备。

如果您和家人之间有持续的、对话式的、信任的关系，您可以用一系列较小的谈话向他们解释情况，而不是一次长长的坐谈。评估您会有多少时间和可以获得多少注意力。

对发生的事坦诚相待是值得的。这可以帮助建立更强大的关系，并消除那些常见的神秘感，同时鼓励其他没有考虑到这种情况可能发生在他们或他们认识的人身上的人认真对待网上隐私。大多数人都会以恐惧和同情来回应，尽管有时他们会建议甚至坚持让你报警。

与您的朋友和家人交谈时要记住这些事：

- 人肉狂的目标是让你的人际关系紧张，毁掉你的生活。不要让他们成功。告诉你的家人，支持你的最好办法就是拒绝屈服。

- 不要声称自己是无缘无故的目标，人肉狂对你的迫害正是源于你的反抗信仰，你应该公开承认这点。如果拒绝承认，只会使那些无法与反抗政治保持距离的人失去合法性，并进一步危害他们。

- 不要让任何人将发生的事归咎于你。为一个更美好的世界而战就必然涉及到挑战，如果说你的努力引发了这种反应，那是你

的功劳。请为此骄傲。

- 提出你可以帮助同伴了解情况和保护自己的具体方法。把这篇文章和相关资源清单给你的同伴；如果他们不懂技术，你可以帮助他们。

- 告诉他们可以做出什么准备，准确地告诉他们会遭遇什么。让他们做好最坏情况的准备，但要强调那并不是绝对可能发生的。

- 要清楚你需要他们提供什么。

[image]

不要妥协，继续前进

深吸一口气。不要责怪自己。在情感上，这可能会给你带来深深的困扰和破坏，给你的生活增加一层急性压力。有时，如果你的名字被 google 搜索到，来自 doxxes 的信息就会成为互联网的永久部分；这可能会影响你的工作前景。

在您确定自己在聚光灯下的时间已经结束之前，您可能不得不改变自己生活的某些方面。问问自己："我想过什么样的生活？我怎样才能控制自己的焦虑？我是否有办法可以接受自己成为一个更加公众的人物？我怎样才能放心地去冒险，重新活跃起来？"特别是，随着政治紧张局势的加剧，采取更极端的安全措施可能是重要的。

以下是您可能选择采用的一些措施：

- 不要让任何人给你拍照，除非你非常非常信任他们、并以你需要的方式处理图像。这可能会造成一些尴尬的对话，特别是在家庭活动或职业场合。注意谁会出现在与你的照片中；告诉他们，与你一起出现在照片中可能会引起不必要的危险。排练一下你可能需要进行的对话，会很有帮助。

- 在家中和敏感的工作地点安装摄像头，尤其要注意摄像头的安全性！

- 保存你所经历的所有骚扰的日志。

- 如果你搬家，切勿公开更新你的地址。不要登记，因为这会使你的地址被记录。尽量保留你的旧驾照或身份证，并在邮局信箱里接收邮件。考虑什么时候使用真实地址，什么时候使用假地址，或者在网上或现实中报名时完全省略地址。

- 如果需要，在网上和现实中使用假名。不要反复使用同一个假名。

- 当你去参加行动时，特别是当你不蒙面时，要注意哪些团体、地方或个人可能会因为在你附近被拍摄到而受到牵连。

- 投入时间参加自卫课程。这可以包括武器训练，但必须包括防卫和解除武装训练。 BACK **[image] S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训** ；**[image] S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法**

- 去看心理医生或者获得社区专业心理协助，以克服您所经历的任何创伤。 BACK [image]S08精神心理安全-总章节：唤回心灵

- 帮助您的朋友和家人了解网络安全的重要性。

- 与您的政治亲和力圈子以外的人进行坦诚的对话。您可能会惊讶于他们所表达的同情心。

无论针对您的人如何努力让你感到孤立，您都不会真正被孤立，一定要信任这点。

作为一个社区，我们必须保护彼此和我们的在线网络免受骚扰、监禁、政治暴力和恐吓。

团结起来，我们就能做到这一点。

[image]
[image]

泄漏文件显示间谍已经能绕过 **Signal** 的加密，那么端对端还有用吗？

[image] 关键词	操作安全性 端对端加密 自卫
[image] 关联	[image]如何才能安全地使用端对端加密（比如Signal）：准则；[image]数字技术限制和最佳实践
[image] 创建时间	2021年3月24日
[image] **Description**	操作安全性

端对端加密的确可以被绕过，但不是那么容易被破解。

- Table of Contents

  弱点**1**：端
  弱点**2**：有针对性的监视
  弱点**3**：元数据
  所以 **...**
  静态加密

[image]

由于美国对WL创始人的起诉，一些中国朋友再次谈及WL曾经发布过的经典文件，其中之一就是 Vault 7；这套泄漏文件的确非常惊人，它展示了中情局的黑客工具无孔不入的危险程度。

对于普通互联网用户来说，该文件中提示的技术工具引起了一个争议——“如果间谍已经可以入侵端对端加密应用，那端对端还有用吗？”

如果您自2013年5月以来在任何时候使用过互联网，您可能都听说过这样的建议：要使用加密通信。斯诺登揭露的大规模监视显示间谍机构一直在记录所有人的电话、短信和电子邮件，这引发了加密应用和服务的开发和使用的激增。

仅仅几年后，加密技术就被广泛用于日常通信，这是斯诺登带来的最明显变化之一，虽然监视本身并没有被阻止。

如果您使用这些加密工具，可能也听说过“端到端加密”或“E2EE”这个词。这个概念很直接：端到端意味着内容从一个端点（通常是你的手机或电脑）到另一个端点（你的信息的预期收件人的手机或电脑）进行加密。但这对于我们这些用户来说，它承诺的安全程度究竟如何呢？

自特朗普执政以来，美国海关和边境保护局（CBP）加强了对旅客隐私的侵犯。CBP一直要求搜查美国公民和所有游客的手机和笔记本电脑，他们还要求旅客提供密码或登录个人的社交媒体账户，以允许当局搜查。不遵守的旅行者将面临被拒绝入境的威胁。

2017年3月7日，Wikileaks 公布了大量泄露的中情局文件 Vault 7，包括中情局花钱买来的漏洞和漏洞知识，并对公众保密。现在这些信息已经泄露，知道这些漏洞的不再只是中情局，而是所有人。

换句话说，您的对手不再只有那些间谍，而是知道怎么使用这些技术的任何坏蛋。

然而《纽约时报》和其他主流媒体的报道对此的解释是错误的，他们说，“中央情报局破坏了 Signal 和 WhatsApp 等应用程序中的加密”，而实际上，中央情报局所做的是针对性地损害了特定人群的 Android 设备。

简而言之，这一揭露反而证实了使用端到端加密通信的重要性，它阻

碍了国家层面的行为者进行大规模监控的能力。E2EE仍然很重要。

有关 Vault 7 的许多媒体解读给人的印象是，诸如 Signal 之类的加密应用已被破坏。而实际上，入侵是在设备级别上的 —— 也就是“端”。没有理由相信加密本身不起作用。

那么，危险在哪里？

[image]

弱点1：端

首先，重要的是要明白，如果你能读到一条信息，那就说明它是明文 —— 也就是说，不再是加密的。通过端对端加密，安全链中的薄弱环节就是你和你的设备，以及你的收件人和他们的设备。如果你的收件人可以读取你的信息，任何可以访问他们设备的人也同样可以读取这条信息。

一个卧底警察可以偷窥你的收件人的手机以读取你发送的信息 —— 比如肩膀冲浪，或者警察可以没收你的收件人的设备并将其破解。如果这些风险中有任何一种可能发生，你应该在发送任何你不想与政府间谍分享的东西之前三思而行。

思考方式至关重要！安全不是一个人能完成的工作，也不是哪个软件能帮您做到的，您需要科学的协作才能真正获得安全

“Vault 7” 的泄漏恰恰证实了这点，它展示了如果你的对手（如CIA）获得了你的电子设备、或你的联系人的电子设备的物理访问权限，并能够解锁它，像 Signal、WhatsApp 和 Telegram 这样的应用程序就完全没用了。

围绕 Vault 7 的许多报道都有些误导性，给人的印象就像是这些加密应用本身已经受到了损害。事实上不是，在这种情况下，妥协是在设备层面 —— 也就是端 —— 发生的。加密本身仍然可信。

弱点2：有针对性的监视

考虑到您很可能无法控制您的联系人的安全状况，您应该考虑到：您发送给对方的任何信息都有可能被间谍阅读。

如上述，肩膀冲浪和被警察查抄手机，这两种情况可能更多见一些；比如，你的联系人在接收你发送的信息的时候正在乘坐电车、正坐在咖啡馆里、或者在机场大厅的长椅上等等，监视者可以近距离偷窥此人的手机屏幕，这就是肩膀冲浪；并且，在美国和中国，都有很多警察查手机和电脑的情况，您应该知道如何随时防御这种状况 —— 这是彻底毁掉端对端加密的手段。

[image]

返回：[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

返回：[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

返回：[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法

但以上这些并不是全部危险性，还有一种如今越来越多见的情况，就是 —— 恶意软件；也就是说，您的联系人的电子设备已经被恶意监视软件感染，而对方不知道，这类恶意软件可以记录目标设备上所有传入和传出的通信。

当然，感染者也可能是您自己。

这种妥协的功能也是在端级别的，它可以使 E2EE 完全失效。因为很难知道您自己（或您的信息接收者）是否是这种类型的攻击目标，所以，最好的办法是 —— 默认不要通过任何数字通信发送过于敏感的信息。

弱点3：元数据

关于端对端加密，您应该知道的第三件事是，它不一定能保护您的元数据。

根据通信的传输方式，日志仍可能显示通信的时间和长度，以及发送者和接收者都是谁。日志还可能显示通信时发件人和收件人的地理位置。

虽然这通常不足以让某人单独入狱，但是，在证明人与人之间的关联、确定与间谍感兴趣的地点（比如抗议现场）的接近程度、以及追踪通信模式方面，它是非常有用的。所有这些信息都有助于在直接监视的情况下建立更大的目标行为模式。

所以 ...

如果端到端加密不一定能保护您的通信内容，而且还放弃了非常有用的元数据，那么使用它的意义何在？

E2EE 做的最重要的事之一就是：确保您的数据永远不会以可读的形式进入别人的服务器。由于端到端加密从您点击 “发送” 的那一刻起就开始了，并且一直持续到收件人的设备上，因此，当一家公司（如 Signal）被传唤到警察局以索取您的通信记录时，他们没有任何明文内容可以交给警察。

这就使当局处于这样的境地，即：如果他们想获取您的通信内容，就不得不花费大量的时间和资源来试图破解加密。在美国，您的快速审判权可能会使这些证据对检察官毫无用处，因为检察官无法迅速解密以取悦法官。在中国，他们可能无限期关押您，而没有任何证据，这期间抗议者可以采取行动给当局施加压力，要求释放您。和国际上的权利组织联合效果会更好。

E2EE 的另一个用途是让间谍部门的大规模监视项目变得更加困难。由于传输过程中没有任何一个点可以抓取您的未加密通信，所以任何抓取所能获得的都是同样的加密文本块，当然这可以通过法庭传票获得。

大规模监控一般是通过收集任何可用的数据，并对其进行自动排序而不是单独分析。使用加密技术可以防止对内容进行算法筛选，从而使这一过程变得更加困难，通常间谍部门会认为这个时间浪费得不值得。

除了大规模数据收集外，间谍和警察还经常使用被称为 [image]黄貂鱼 的手机站点模拟器。黄貂鱼假装成手机信号塔，以欺骗您的手机连接它，使其放弃可识别性信息，包括您的位置。

黄貂鱼也会抓取并记录您的所有通信。与其他拦截方法一样，加密意味着被间谍检索到的信息基本上是无用的，除非这些间谍愿意花大力气去解密它。

静态加密

除了使用端到端加密来保护正在发送的信息内容外，您还可以使用全盘加密来保护存储在设备上的信息。

适当的全盘加密意味着，如果没有您的加密密钥（通常是口令），您设备上的所有信息都无法破译，从而创建了一个更难入侵的加固端。

虽然全盘加密不一定能防止一些更隐蔽的监控方法，如恶意软件，但它可以防止获得您的设备的警察和间谍从其中提取任何有用的数据。这种提取通常被称为 “取证”（挺讽刺的），您可以在下面看到详细解释和防御方法：

[image]

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些

数据？

返回：[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

返回：[image]在雷达下低飞：变得难以被追踪的简单方法 S03E07

返回：[image]与S先生共度美好一天-变得难以被追踪的简单方法 S03E03：反取证技巧

端到端加密绝不是抵御民族国家监视或恶意个人监控的神奇盾牌，但 **Vault 7** 强调了使用它如何帮助迫使程序从大规模监控模式转向资源密集型目标攻击模式 —— 简单说，如果您不是如斯诺登那样的被全球通缉的“要犯”，那些间谍很可能就不会愿意把大笔的资金花在您身上。

当与良好的安全意识、加密设备、和其他安全实践相配合时，E2EE 可以成为一个强大的工具，显著减少您的攻击面。始终如一地习惯性地使用端到端加密，可以使许多较低级别的威胁失效，甚至可能使一些更高级别的对手决定攻击你太费劲了，根本不值得。

就如我们强调的安全宗旨 —— 不要相信任何**100%**安全的承诺，那绝对是骗子，真正有效的防御是，为自己争取到足够的时间，尽可能消耗监视者的金钱和资源，让他们因玩不起而放弃追踪您。

并且，切勿小看任何传统的、似乎落伍的间谍手段，当大多数人都把注意力放在那些最新出现的高端的间谍手段上时，反而容易在套路上中招。

[image]
[image]

如何才能安全地使用端对端加密（比如Signal）：准则

[image] 关键词	人际安全 关系 端对端加密 预防性
[image] 关联	[image]数字技术限制和最佳实践；[image]泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？
[image] 创建时间	2021年3月25日
[image] Description	操作安全性

一个软件不能保护您的一切，最严重的问题往往都出在人身上。

- Table of Contents
当创建一个新群组时
担保
使用担保的一些标准包括：
规则
签入政策

[image]

您应该使用端对端加密，这不必细说了；幸运的是如今很多人已经理解到使用端对端加密的重要性，尤其是，人们已经知道，安全不是哪个软件能完全解决的问题，安全必须是一套科学的思考方式 ➕ 科学的操作方法 ➕ 有效的协作。

[image]

准备获得系统性的入门级培训体验的用户请从S01进入：[image]S01 整体安全 - 总章节：前线安防入门课

Signal 也一样。作为一个安全工具，如今它是许多群体相互联系和沟通的首选渠道。用户团体的意图和目的可以有很大的不同，从制定晚餐计划到组织下一次反抗运动。

但仅仅使用 Signal 还不足以保证您和您的朋友的安全 —— 安全只有在堵住最薄弱环节之后才能有保障，在通讯软件上，“最薄弱环节” 就是：您与之交流的所有人中最不注重安全性的那个/那些人。

因此本文将概述一些准则和协议，以帮助加强您的个人和集体安全实践。

请注意：端对端加密工具不只有**Signal**！本文中强调的大部分准则适用于所有端对端加密通信应用。

当创建一个新群组时

加密通信的技术能力本身会给人们一种误解，似乎 “我终于可以随便说话了”，并不是这样的！还记得英国间谍搞出来的入侵 Signal 的方法吗？是的，最危险的部分在于人。 BACK [image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

创建群组要有目的性，添加成员同样需要有目的性。在将任何一个人添加到您的联系人列表之前要知道：一旦某人成为群组的一部分，您就不可能简单地将其删除了。您不可能在完全放弃这个群组或者要求此人离开之前删除他。

您随时应该知道您加进来的人都是谁。

考虑一下您会怎么处理一个一开始就被单方面添加进来的人，单方面添加指的是比如无法双向认证的，或者是让群组中其他人对此有顾虑的。另外，在没有事先征得群组中其他人同意的情况下，不要把新人加到敏感的群组里。

群组建立后，您需要说明此群组的目的，并立即点名 —— 可以完全根据您的需求，不论是不是实名，或所有成员都使用代号，只要彼此知道谁是谁就可以了。这些应该在对话开始之前完成。

不要在没有问过群组成员的情况下添加新的人进入，并给人们一个指定的时间来表达意见，比如24小时，因为许多人不可能每时每刻都在手机上活动。鼓励原成员对新成员提出问题或进行阐述，这比简单地说 “您担保” 更有助于创造良好的对话。

每次增加新成员时，都要重新点名，这样您的群组其他成员就会知道自己正在和谁说话。

担保

这里的的担保就是它本来的意思 —— 即 支持是真实的、确定的、可靠的，或 证明、保证、认证。在政治背景下，为某人担保指的是，您相信此人致力于团队的目标，值得信赖，可靠和负责任。

[image]

返回：[image]“我的”朋友还是“我们”的朋友？：如何执行担保措施

请记住，担保是对您个人意见的反映，建议谨慎使用担保，因为如果是不负责任的担保，就会影响群体的安全、信任和凝聚力。

担保是某人获得一种凭证，这样的 “凭证” 对于以前可能没有合作经验的群体来说非常重要，他们需要一定的信任和安全感才能舒适有效地合作。

担保制度可以让1个人或多个人（越多越好）使用他们从团体中获得的信任，并将其扩展到他们想要带入的人身上。担保的必要性根据您工作的内容而异，越是敏感的工作，这个过程就越是需要谨慎。

担保某人是否应该能够进入一个群组的对话、是否合乎该群组的目标和目的，应该结合群组的整体目标和风险来考虑。群里的其他成员在选择是否相信您提供的担保时，都会有自己的判断力。

使用担保的一些标准包括：

- 认识此人有一段时间了，对此人有一定程度上的了解；尤其是，了解此人在该群组的目标方面的契合度；

- 您与此人合作过一段时间，对此人的工作方式、品格和原则立场有一定了解；

- 您的熟人中有一些人在一定时间内与此人合作过，他们对此人的信任加之您对他们的信任，可以在您的心目中给此人一个信任度的基础分数；

- 您了解此人的优势和缺点，以及知道此人在面临镇压的情况下的反应；

- 您知道此人如何回应批评或反馈，以及此人对自己的行为负责的程度；

- 您了解此人的大家庭、儿时的朋友、以及整个人生故事（开个玩笑…也许是，但比较少见…）

总之，您应为以下人员提供担保：您认识和信任的人，您知道他们了解特定群体的目标和安全要求，您知道他们参加过专业的扎实的安全培训，并可以熟练使用安全操作。

您不应该仅仅因为 “知道这个人的存在和其工作内容” 或 “有过一两次愉快的谈话” 就给予此人担保，虽然这些东西是了解和信任某人的一部分，但它仅仅是一部分！并非全部。

担保的严格程度会根据你们的对话的敏感度和团体承担的风险等级而有所不同。如果这是你没有考虑过的问题，现在就需要考虑（我们在不久后会更详细介绍安全文化的构建）。

[image]

无论您用什么标准来担保他人，都要提前跟群组里的每个人沟通，而且每个人都需要站在同一条线上。担保这个词已经被用烂了，几乎没有详细地说明，人们对它的含义往往有不同的想法。这就是您需要沟通的地方，让所有人统一对这个概念的理解标准。

请注意，数字安全不能代替关系安全！如果您决定信任的任何一个人在敏感的信息对话中，结果此人本来是恶意的、鲁莽的、粗心的、或不负责任的，那世界上所有安全软件和安全协议都无法帮助您。

[image]

规则

当重新安装 Signal 或获得新的电话号码时，请事先通知各群组，让他们知道要接受新的安全密钥 —— 他们会看到您的 “安全码已改变” 的提示，如果他们不知道您在做什么，他们会因此害怕。

或者，如果您无法事先通知其他人，也要在事后立即让他们知道。根据安全级别不同，您应该选择亲自见面、或发送安全号码的截图，来验证新的安全码。

使用安卓系统时，一定要在 Signal 应用上设置密码和超时功能。可惜iOS还没有这个安全功能。至少要为整个手机设置一个复杂的字母数字密码。从法律的角度来看，形状、图案和拇指指纹/生物识别技术都是不安全的，维稳官员可以依法强制您出示指纹来解锁手机。此外

也要对您的手机进行加密。

一定要使用阅后即焚。时间设置长短根据您的具体危险状况来判断，您需要想象威胁会如何发生，据此来判断多长时间的销毁是合适的。如果您的群组中任何一个人的手机被警察抢走，却没来得及锁屏，你们所有人都会被暴露。

并且，您需要时刻关注阅后即焚时间的稳定性，有时，当群组中有人重新安装应用程序或添加了新的人员进入时，阅后即焚可能会被自动关闭。您需要确保及时地重新激活该功能。

如果您正在参加反抗行动、或处于可能导致逮捕的任何一种情况下，包括过境，而您又带着手机，请事先离开所有的群组并卸载 **Signal**。不论如何，建议不要把您的个人手机带入上述这些情况中。

[image]

在本站的 ❤🔥行动安全性-OPSEC 专题中查看更多相关具体说明。

如果您在跨越国界，必须首先离开所有群组，并卸载 **Signal**。因为通常保护您免受搜查和扣押的法律基本都不适用于国际边境。如果您在国外旅行，强烈建议不要携带您自己的手机/平板电脑/笔记本电脑/等。

如果出现安全漏洞，比如您带着手机被警察抓到，或者您的家被警察突袭，您需要指定一个人开始一个新的群组，并立即离开旧的群组（也就是烧掉这个群组）。确保威胁不会转移到新的循环中。指定一个人留在旧群组上，确保所有人都完全离开了。最后删除这个群组。

在手机丢失/被盗或被警察没收的情况下，立即向与您在同一个群组中的其他人报告，让他们提醒所有成员需要抛弃旧群组并重新开始。

[image]

激进社区用户请从这里进入：[image]防篡改准备 ；[image]物理入侵检测 ；[image]突袭应对措施 ；[image]镇压应对措施

签入政策

有些群组是短暂的，是为了特定的短期目的而存在的，在目的完成后应予以删除。生命期不确定的群组应定期检查成员情况，以帮助消除松散的问题。

考虑建立签到/参与小组讨论的制度。要求群组成员定期重新判断自己在邮件列表或名单上的兴趣，并确保没有出现安全问题。有些群组也可以选择对成员实行定期签到的要求 —— 如果在某段指定时间内没有收到某人的签到，可能表明存在安全漏洞。这在那些经常出现强迫失踪的国家来说，是很有必要的，如果您的群组成员被失踪，您需要做最坏的考虑，尤其是需要及时知道这件事。

[image]

请记住。有时即使一个成员离开了群组，他们也会继续收到该群组的消息（由于软件故障）。如果该群组的信息是敏感的，某人离开此群组应被视为安全漏洞，该群组应立刻被烧毁。重建。

讨论敏感资料 —— 不论是过去的、现在的或将来的 —— 应该只在所有成员 *需要知道* 的基础上进行，而不是 “我相信你” 或 “我觉得这个很酷”。吹嘘、八卦和传言都是危险的行为，在您的行动中应该没有地位。

尤其是！具体的行动规划讨论应该面对面地进行 —— 决不要以数字方式进行！所有的数字安全都有弱点和漏洞。您越了解数字安全的弱点和局限性，您就越能保护自己。

[image]

激进社区用户请从这里进入：[image]户外无设备对话 ；[image]关系网络图谱

[image]
[image]

什么是凭据填充攻击？如何选择密码管理器？

[image] 关键词	个人 威胁模型 密码 密码管理器
[image] 关联	[image]数字技术限制和最佳实践；[image]硬件密码管理器；[image]一次性密码和2FA应用 [image]一句话安全须知：记住这些句子，以简单地优化您的安全性
[image] 创建时间	2021年5月21日
[image] **Description**	操作安全性

数据泄露经常发生，无法避免；最重要的是，您需要随时保护自己，将可能的损失降到最低。

- Table of Contents

  什么是凭证填充？
  填充攻击是如何进行的？
  填充攻击如何逃避检测？
  凭证填充攻击和暴力攻击之间有什么区别？
  凭证填充和凭证转储有什么区别？
  如何保护自己免于凭证填充攻击？
  如何安全地使用密码管理器
  1、离线密码管理器
  2、在线密码管理器
  3、无状态密码管理器
  哪个密码管理器系统是最好的？

[image]

凭证填充攻击是一种网络攻击形式，涉及将偷来的凭证 “填充” 到多个网站。

像机器人这样的工具可以让攻击者进行自动填充，让他们可以在短时间内针对几十个网站测试数百万个登录凭证。

以下是您需要知道的关于这种攻击的内容，尤其是，您可以保护自己的简单方法。

什么是凭证填充？

凭证填充是指将大量被盗的密码和用户名塞入多个网站。攻击者依靠在暗网上兜售的庞大的泄漏数据；他们的目标是利用以前泄露的数百万个登录名和用户名组合来渗透到其他网站。

攻击者之所以能成功，依赖的是一个普遍存在的人为错误 —— 即 在多个网站上使用相同的用户名和/或密码。根据研究，高达85%的用户在不同账户上循环使用密码。

而正是这种人为错误，让攻击者可以利用一个网站泄露的登录凭证进入其他网站和服务。

成功率相当低，只有0.1%到2%左右。这意味着，每测试一百万个登录凭证，只有大约1000个凭证可以用来进入其他网站。但是，让攻击者的努力变得值得的是，他们可以将每一个被他们成功渗透的账户变成收集数据的金矿。

假设他们设法入侵了大约1000个账户，这些账户都有银行信息或信用卡凭证，他们就可以抽走资金或利用这些信息进行其他形式的欺诈。其他个人身份信息(PII)，如 身份证号码或税务信息，可以用来实施犯罪，如身份盗窃 —— 就是用您的身份干坏事，让您背锅。

攻击者会将他们在每个账户中发现的任何信息货币化，这使得尽管登录凭证即便匹配率很低，攻击也是很值得的。

填充攻击是如何进行的？

当然，攻击者不会手动将偷来的登录凭证逐一输入不同的网站，因为他们需要数以百万计（甚至数十亿计）的偷来的登录凭证才值得进行攻击。

相反，这些泄露数据会被加载到僵尸网络中，发起自动登录尝试。然后，他们会使用进一步的工具来逃避检测。

一个僵尸网络每小时可以进行数千次登录尝试。例如，2016年的一次凭证填充攻击使用的僵尸网络，每小时在多个网站上发送超过27万次登录请求。

填充攻击如何逃避检测？

虽然许多网站使用安全措施来检测恶意登录尝试，但黑客已经找到了规避这些措施的方法。

一个代理列表被用来反弹请求，并掩盖源头，或者简单地说，使登录请求看起来像是来自不同的位置。他们还使用其他工具，使其看起来像是多次登录尝试来自不同的浏览器。

这样做的原因是，只来自一种类型的浏览器的多次登录尝试（例如，每小时一千次）看起来很可疑，并且有更大的机会被标记为欺诈。

所有这些技术都可以模仿不同地点的数千名用户的合法登录活动。这使得攻击向量变得简单，但却很难被发现。

凭证填充攻击和暴力攻击之间有什么区别？

凭证填充是暴力攻击的一种子类型，因为它更有针对性，所以更有效。

暴力攻击本质上是使用不同的随机字符组合来猜测密码。他们使用自动软件通过测试几种可能的组合进行多次猜测，直到发现密码。

另一方面，凭证填充使用以前数据泄露的登录细节和密码。他们使用一个网站泄露的密码-用户名对，然后在其他服务上进行测试。

虽然使用强大的密码可以保护您免受暴力攻击，但是，如果您在其他网站上使用相同的密码，当填充攻击发起时，您就会中招。

凭证填充和凭证转储有什么区别？

虽然看似相同，但凭证转储是一种不同类型的攻击，针对一个入口点或机器来渗透网络。

凭证填充使用以前泄露的多个登录凭证进入其他网站，而凭证转储则是进入一台机器并提取多个登录凭证。

这是通过访问计算机许多注册表中的凭证缓存或从安全帐户管理器（SAM）数据库中提取凭证来实现的。后者包含所有创建的帐户，密码保存为哈希值。

凭证转储攻击的目标是获得进入网络的立足点或进入系统中的其他计算机。在从一台机器上提取登录凭证后，攻击者可以重新进入设备或进入整个网络造成更大的破坏。

与填充不同的是，凭证转储攻击是利用一个入口，一台存在未修补漏洞的机器来渗透整个网络。

如何保护自己免于凭证填充攻击？

对于大多数用户来说，最好和最简单的保护自己的方法是对每个网站或账户使用独特的密码。至少，对于那些有您的敏感信息的网站，必须要这样做。

启用双因素验证（2FA）或多因素验证（MFA）有助于使攻击者更难接管账户。

如果您发现记住多个密码和用户名很混乱，您可以使用一个可靠的密码管理器。如果您不确定它们的安全性，请查看下面的密码管理器使用的安全方法。

或者尝试一个开源的密码管理器。比如，KeePass Password Safe、Bitwarden、Passbolt、Psono、Teampass。

[image]

如何安全地使用密码管理器

密码管理器有几种，您可以对比一下根据您的具体情况选择。

1、离线密码管理器

[image]

在电脑上运行的密码管理器应用程序必须将您的密码保存在某个地方。一种方法是将这些信息放在电脑上的一个文件中。由于这个文件包含非常敏感的数据，任何一个像样的密码管理器都会确保对该文件进行加密。

加密后的数据并非无法完全破解，但对于大多数人来说，这是一项很

难完成的任务。另外，它需要的时间真的很长。大多数盗贼不会费心费力去做这种事。即使是警察部门和政府间谍也会觉得这个任务非常艰巨。但只要有足够长的时间和非常大的意愿，还是可以做到的。

因此，虽然您的数据并非坚不可摧，但很可能是安全的，除非您做了一些惊天动地的事，让自己成为间谍和警察认为的 “值得努力的目标” 。

如何获取您的数据？最简单的方法是主密码。您的密码管理器会要求您创建一个解密文件所需的密码，就如一个金库，其中包含了您所有其他密码。

您可以通过要求提供密钥来使这个金库更难被破解，密钥是一个存在于电脑或U盘等单独设备上的隐藏文件。

优点：

- 提供最大的控制力和灵活性
- 只有您知道您的数据存储在哪里

缺点：

- 可能需要更多的技术知识
- 最不适合多设备使用

当您把所有的密码都放在一个地方时，您就创造了安全专家所说的单点故障。就如您把所有的现金都存放在一个金库里，那么有人只需要瞄准一个地方就可以拿走您的全部财产。如果您把密码存储在不止一个文件中，那么就会增加盗取您所有数据的工作量。

您可以通过加密并将每个密码存储在自己的文件中，使攻击企图更难

完成。您可以使用Pass密码管理器来实现这一点。

离线密码管理器往往是免费使用的。有些可能有需要额外付费的功能。Enpass 是下面唯一有付费选项的。

Download: **Keypass** (免费)

Download: **Password Safe** (免费)

Download: **Enpass** (免费下载，应用内交易)

Download: **Pass** (免费)

2、在线密码管理器

密码管理器已经存在了很长时间，但在过去的十年里，人们上网的方式已经发生了变化。许多人不再有一台主要的电脑。现在的人们经常有许多设备，并且很可能从手机和笔记本电脑上登录自己的银行账户。

有了多种设备，密码管理器可能会带来挑战。如果您的口令都存储在一台电脑上，并且是随机生成的，您既不能在另一台设备上访问它们，也难以记住它们来手动输入。在某些情况下，您可以同步您的密码，但如果不存在兼容的移动应用程序，您就麻烦了。

进入在线密码管理器。这些服务将您的凭证存储在网上，您可以从多个设备访问它们。

但是，基于互联网的密码管理器有一个很大的漏洞。您的一切密码现在都可以在线获取。如果有人能够访问这些数据，他们就可以冒充您，控制您的账户，并窃取您的金钱和身份。这就像有人拿到您家的门钥匙、钱包和社保卡一样糟糕。

为了降低风险，服务会先对设备上的密码进行加密，然后再将数据上传到网上。但并不是所有的服务都以同样的方式处理和保护这些数据。如果您忘记了您的主密码，他们是否有能力重置您的主密码？他们是如何处理安全问题的？事先了解这一切。

为了方便起见，网站能够帮助您重新获取数据是很好的；但是，如果在该公司工作的人能够做到这一点，那就意味着入侵者也可以做到。这些公司还经常添加额外的功能来吸引用户，最终会让您的数据面临更大的风险，比如自动登录网站。

优点：

- 使用最简单
- 同步是自动的
- 支持最广泛的设备数量

缺点：

- 您的数据是在线存储的
- 一些便利的功能只会让您的安全感降低
- 许多功能都要花钱

在线密码管理器是最商业化的。虽然很多都是免费使用的，但它们通常会为付费用户保留某些功能。有些服务根本需要付费才能使用。

Download: LastPass (免费)

Download: Bitwarden (免费)

Download: Dashlane (免费)

Download: 1Password (免费下载，付费使用)

3、无状态密码管理器

即使有加密功能，使用上述任何一种方法都意味着创建一个以前不存在的密码记录。这不是您使用密码管理器可能承担的唯一风险。这样的因素会让人对使用密码管理器的想法特别反感。

但是，有一些密码管理器并没有将您的密码的加密副本到处乱放。取而代之的是，它们会根据简单、易记的变量生成密码。一种常见的方法是使用您的主密码和网站名称的组合来创建密码。

每次输入这些信息，您都会得到相同的密码。

即使攻击者知道您使用的是哪种程序和底层算法，他们仍然需要您的主密码、网站名称和密码的长度来复制您的安全密钥。另一方面，如果有人破解了一个账户，并找出了您的主密码，那么他们就有可能在不需要破解任何形式的金库的情况下，找出您所有的其他密码。

优点：

- 没有密码库需要保护
- 无需同步数据

缺点：

- 没有办法注意到有异常密码要求的网站

- 没有简单的方法来处理您不得不更改密码的网站。

无状态密码管理器往往是开源项目，您可以免费下载。

Download: **PwdHash**

Download: **SuperGenPass**

Download: **LessPass**

Download: **HashPass**

哪个密码管理器系统是最好的？

一个只存在于桌面上的密码管理器是很好的，但如果您采取快捷方式从手机或库登录，就可能会留下漏洞。在线密码管理器可能更方便、更直观，但您的密码还是在别人手里。您该怎么做呢？

没有所谓的完美安全。如果您是在最隐秘的条件下工作，也许应该选择保存单独的密码库，所有的关键文件都用不同的U盘来保护。听起来好像太麻烦了？即使您的技术经验仅限于知道如何使用电子邮件和社交媒体，您也可以很容易弄清楚 LastPass 或 1Password。

这些选项中的任何一个都比重复使用相同的几个密码更安全。一旦您开始使用密码管理器，就已经在反击攻击者了。

[image]
[image]

社交媒体上的行动主义安全性:框架手册

[image] 关键词	社交媒体 自卫
[image] 关联	[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗 ；[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式
[image] 创建时间	2021年7月1日
[image] **Description**	操作安全性

如果您必需使用社交媒体谈论政治和敏感的行动，这里是最基本的您应该知道的事。

- Table of Contents

关于社交媒体平台用户生成的数据相关的四个方面问题：
任何人都可能被入侵，不论您是否信任此人
保护您的设备免受物理威胁——
身份：您在网上的身份与您想让别人了解的您的身份——
在社交媒体上分享图片、视频和文档——
照片：
PDF文件：
文本文件 —— 根据用于创建文件的程序，数据可能包括：
视频 —— 视频文件中的元数据可以分为两个部分：
音频 ——
通信 ——
分享图片的替代方案
社交媒体上的匿名性
真名——

匿名——
假名——
集体身份——
社交媒体的问题
您的身份
与更多公众分享信息
Facebook
推特/**X**
Twitter的替代选择
创建和宣传活动
群组
通信

[image]

本文是框架手册，以最简单的语言描述敏感人士在社交媒体上的安全问题和防御方法；重要部分嵌入了详细介绍。如果您在您的团队培训中讲授本指南的内容，请将其中嵌入的部分展开，做详细讲述。

[image]

最常用的社交媒体平台是沟通、组织、动员和获取信息的有力工具。它们的商业模式是基于集中化的数据囤积、处理和分析。这种史无前例的数据聚合使上述所有好处得以实现，但其副作用是令史无前例的监视、操纵、和网络暴力变得易如反掌。

人们产生的数据往往是极其个人化的—— 我们做的搜索、我们提出的问题、我们说的话或看的东西，这些都会产生数据；但数据也是我们什么时候做的事，和谁做的事，在什么情况下做的事的详细说明。所有这些汇集在一起，就构成了非常强大和有洞察力的私人形象，从社会、文化和政治角度来看，它是关于我们是谁、我们属于哪里、有什么习惯和偏好、甚至内心的弱点。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

数据也是很容易被积累、复制、分享和操纵的东西。通常是为了赚钱或其他利益，如影响力、控制力和骚扰侵犯。

社交媒体平台已经成为公民社会组织（CSO）、草根团体、活动家和相关个人的外联和动员工作的中心舞台。本文将重点探讨社交媒体平台用户生成的数据对公民行动主义的影响。

关于社交媒体平台用户生成的数据相关的四个方面问题：

1、平台和个人数据 ——

对个人活动家和整个行动网络的隐私以及对收集和分享个人数据的关切。除了在线审查之外，在政府要求下或平台自行判断所引发的删除帖子或封锁账户的行为也是如此。您可以在这里看到详细解释 https://iyouport.substack.com/p/lr-2?utm_source=publication-search。

2、当局和个人数据——

根据活动家和组织在社交媒体上的分享内容锁定目标；诽谤；通过法律行动从平台上获取个人信息；在某些情况下，使用暴力获取密码，以解锁用户账户及其社交圈的信息。

3、对手和个人资料——

通过诽谤活动，传播虚假信息，泄露个人照片，以及通过像“人肉”这样的攻击，可能造成非常严重的后果。

4、个人背景和个人数据 ——

由于与家庭或雇主的政治观点不一致，对个人关系、甚至生机所造成的影响。如今这个问题也越来越严重，https://iyouport.substack.com/p/c6a。

要开始对您的数据进行更有战略意义的思考，并对现有的担忧做出回应，重要的是首先要确定威胁和脆弱性，这些威胁和脆弱性可能会根据您周围的环境和政治背景而有所不同。具体做法您可以参见[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性

任何人都可能被入侵，不论您是否信任此人

即使您信任与您分享信息的人，如果您使用的社交媒体/通信软件创建了用户可访问的记录（比如您可以看到过去的活动或信息历史记录），如果其他人获得了与您联系的人的设备或账户的访问权限，您认为可以保持隐私的信息和图像就会因此被泄漏。

还记得卡舒吉是怎么死的吗？那些间谍并没有直接针对他本人，而是入侵了与他联系最为密切的一位朋友的手机，从而曝光了卡舒吉的加密通信内容。只因为这位朋友在网上买了一罐蛋白粉，最终导致卡舒吉被分尸。

攻击往往都采用这种 “旁路” 的方法，因为被列为攻击对象的敏感人士大多学习过如何注意保护自己的隐私，但是他们很可能无法控制与他们联系的其他人，尤其是年纪较大的家人，于是攻击者就会从这里入手。

[image]

我们所有人都是被联系在一起的。好的方面是，我们拥有彼此，联合的力量会很强大；而坏处是，这意味着发生在一个人身上的事，比如账户被黑，就会影响到我们其他所有人。您可以对自己和团队负责，在自己的账户上使用强大的密码，并设置双因素身份认证；但您也需要与您的朋友、亲密队友和社区讨论这对我们所有人的影响，以及他们可以做些什么。

帐户被黑客攻击有可能不是您的错，即使您非常负责任，也可能会发

生这种情况。如果发生了，请善待自己和其他任何人，并专注于恢复而不是责备。如果您的账户被黑客攻击：尝试重新获得访问权，并立即更改密码和其他任何可能使用了相同密码的其他账户的密码；并让您的重要关系网络中的所有人知道您的账户被黑客攻击了，信息可能已经暴露，您的账户发出的消息可能不是来自您。

保护您的设备免受物理威胁——

在很多国家和某些情况下，您的对手可能会采取物理攻击的方式来获取数据。这可能包括盗窃、警察突袭，甚至是通过人身暴力来获取设备。然后使用取证软件获取设备中的信息，包括您以为已经被删除的信息，都可以提取。

[image]

返回：[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

返回：[image]与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧

返回：[image]数字取证

返回：[image]网络取证

返回：[image]计算机和移动设备取证

身份：您在网上的身份与您想让别人了解的您的身份——

关于您的在线行为建立的数字档案，不仅仅是基于您发布的文章或分享的内容或上传的照片；您的数字阴影覆盖面很大，您应该首先绘制它的轮廓，以便了解更多关于您留下的数字痕迹。这将有助于评估有多少关于您的信息，并让您知道从哪里开始更好地控制自己的数据。[image]大清洗 - 扫荡危险区域：完美隐身 S04E07

为此您可以参见 [image]自我人肉 ，以对手的思考方式来验证您自己的薄弱环节，提早弥补。尤其是关于社交媒体情报的应对措施，您的对手很有可能挖掘到您自己都不知道存在的重要信息。

对于您可以采取什么样的身份在线公开自己，这里有一些判断标准您可以参考 [image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

[image]

在社交媒体上分享图片、视频和文档——

当您使用社交媒体平台时，有时您分享的内容远远超过您的想象。这不仅与您分享的数据有关，还与附加的元数据有关。元数据可以理解为传统图书编目的现代版。图书馆抽屉里堆放的小卡片提供了书名、出版日期、作者和在图书馆书架上的位置。同样，在数字领域，一张数字图像中可能包含了拍摄照片的相机、图像的日期和时间等信息，往往还包含了图像拍摄地点的地理坐标。这种与多媒体相关的元数据也被称为EXIF数据。

在实际工作中，重要的是要知道当提到元数据时通常意味着什么。

以下是可能与不同类型的数据一起存储的元数据列表：

照片：

- 如果使用智能手机等具有GPS功能的设备，包含照片拍摄的位置（经纬度坐标）
- 相机设置，如ISO速度、快门速度、焦距、光圈、白平衡、镜头类型等 (请注意，有些相机会包含位置坐标)
- 相机或智能手机的品牌和型号
- 照片的拍摄日期和时间
- 用于编辑照片的程序名称

PDF文件：

- 作者的名字，通常是第一次安装用于创建文件的程序时分配的名字
- 用于创建文件的程序的版本和名称
- 文件标题
- 某些关键词
- 文件创建/最后修改的日期和时间

文本文件 —— 根据用于创建文件的程序，数据可能包括：

- 所有不同作者的姓名

- 文件前几版中已删除的文本和注释行
- 创建和修改的日期

视频 —— 视频文件中的元数据可以分为两个部分：

- 自动生成的元数据：创建日期、大小、格式、CODECS、持续时间、位置
- 手动添加的元数据：关于镜头的信息、文本转录、标签、进一步的信息和编辑说明 ... 等

音频 ——

音频元数据类似于视频，但使用范围更广，特别是用于注册文件的属性。除此之外，它还可以包括：

- 创建日期，大小，格式，CODECS，持续时间和一组手动添加的数据，如标签，艺术家信息，评论，专辑中的曲目编号，流派等。

通信 ——

通信中的元数据取决于所使用的通信类型（如电子邮件、手机、智能手机等）。但在一般情况下，它可以显示以下内容（如果没有使用隐藏元数据工具的话）：

- 发件人和收件人的ID
- 来文日期和时间

- 位置
- 通讯方式…等

您可以关闭手机或相机中的GPS追踪器；还可以在手机设置中限制各种应用程序对您的位置数据、联系人和图片的访问，在这里看到关于权限设置的须知 https://medium.com/@iyouport/%E6%82%A8%E7%9C%9F%E7%9A%84%E7%90%86%E8%A7%A3%E5%BA%94%E7%94%A8%E6%9D%83%E9%99%90%E9%83%BD%E6%8E%88%E4%BA%88%E4%BA%86%E4%BB%80%E4%B9%88%E5%90%97-%E8%BF%99%E9%87%8C%E6%98%AF%E4%BF%9D%E6%8A%A4%E6%82%A8%E5%AE%89%E5%85%A8%E7%9A%84%E9%87%8D%E8%A6%81%E7%9F%A5%E8%AF%86-23d7578d334d。非常建议使用端对端加密通信工具，但必须了解必要的安全文化，并让您的重要联系人都遵循同一套安全文化准则。

在注册设备或软件时，不要使用真实姓名或您在线使用的主要昵称。这样可以防止在使用该设备或软件时创建的元数据与您的姓名或昵称相联系。

在网上发布内容时，您可以将含有大量元数据的文件（如.doc和.jpeg）改为使用较少元数据的文件（如.txt和.png），也可以使用纯文本。

分享图片的替代方案

来自 Guardian Project 的 ObscuraCam 是一款安卓系统的照片和视频应用，可以保护某些信息的隐私。它允许您用像素化、删改（涂黑）或用搞笑的鼻子和眼镜保护可识别部分。

您还可以反转像素化，这样就只能看到您选择的人，背景中的人都无法识别，这在拍摄街头施暴的警察时会很有用，帮助隐藏背景中的其

他抗议者。这款应用还将删除所有存储在照片中的可识别数据，包括GPS位置数据和手机品牌和型号。您可以将受保护的照片保存回图库，或直接分享到 Facebook、Twitter 或任何其他支持 “分享” 的应用程序。

[image]

返回：[image]抗议中谨防常见危险：整体安全 S01E11 - 协作和互助就是战斗力

[image]

社交媒体上的匿名性

对于异议人士和行动者来说，来自家庭和职业圈子的威胁是相当具体的，其影响也各不相同。国家的镇压性法律或社会强加的限制，或活动家的社会或职业网络中的信仰，都可能发挥重要作用。

有两个因素促使活动家注意到所感知的风险。首先，对手可能会拦截活动家的机密数据，这可能导致犯罪或意识形态迫害。

其次是数据足迹带来的意外后果。不论是数据经纪人还是政府，与您的数字活动相关的所有信息都可能会成为监视和针对性的迫害的途径，您很有必要假设数据经纪人能拿到的一切，政府都能拿到。关于他们能拿到什么，以及如何处理这些数据。

这意味着活动家需要小心自己在组织活动时留下的任何数据痕迹，因为今天看似无害的元数据，可能会在未来的任何时候的立法、监管或商业模式下面临危险。

持有与主流价值观不同意见的活动家都会遭到威胁和攻击，在任何国家都是如此，这无需质疑。有些攻击并不需要复杂的技术技能，只需要大量恶意者之间的协调行动；这就是活动家面临的在线骚扰、抹黑运动、恶意举报他们的发布内容和个人资料、人肉、盗用社交媒体账户、身份盗窃和审查网站的方式。

某些类型的攻击需要更多的技术或人力基础设施：恶意软件感染和使用有针对性的间谍软件、互联网搜索引擎中的虚假信息战术、以及克隆在线服务等等，都是很常见的手段。

[image]

返回：🕷人肉搜索

返回：https://iyouport.substack.com/p/as58-

考虑潜在的在线身份如何改善您的安全（以及与您个人和职业相关的人的安全），对于准确评估您的风险，以及安全使用各种在线身份所需的技术技能和能力至关重要。您还需要考虑在特定的情况下，您会使用哪种身份。

以下问题说明了您在评估其他在线身份时应该考虑的因素：

- 如果我的真实身份被人知道，我的安全、工作或生活是否会受到威胁？
- 如果我参与的某些活动被人知道，我的心理健康和/或人身安全是否会受到影响？
- 如果我的真实身份被人知道，我的家人或其他亲人是否会受到任何伤害？
- 我是否能够并愿意安全地保持独立的身份？
- 您需要准确地基于事实来回答这些问题，之后您将看清最适合自己的选择。

真名——

风险：在网上使用您的“真实世界”身份意味着您很容易被家人、同事和其他人识别，而且您的任何活动都可以与您的身份直接联系起来。

声誉：其他人可以很容易地识别您，从而更容易获得声誉和信任。

努力：几乎不需要努力。唯一的问题是，您在现实中掩饰自己多少，在线就需要同样的的程度。

匿名——

风险：它是有益的，但也不容易维持。慎重选择这个选项，除非您具有足够的知识和能力可以保证您的匿名持久性安全。

声誉：需要较长时间的持续努力，因为您需要重建信任和声誉。

努力：需要相当的谨慎和丰富的知识，可能有点辛苦。您必需确定自己可以熟练使用匿名工具（例如Tor或TAILS）。

假名——

风险：假名可能会与您的现实世界身份相联系，但也可以有意地避免形成联系。

声誉：一个持久的假名，别人可以用它来识别您在各个平台上的身份，是获得声誉和信任的好方法。

努力：维护需要一些努力，特别是当您在其他地方使用了真名的时候（非常不建议采取*部分*假名的做法，大致上这和没做一样）。

集体身份——

风险：您的真实身份可能会被集体中其他人的行为所暴露，除非您所在的集体如匿名者组织那样其中每个人都熟知如何保护自己和彼此。

声望：虽然不是获得个人声誉的途径，但您仍然可以从集体的声誉中获益，这往往比个人声誉更好。

努力：中等，重要的努力在于熟悉和遵守共同的《安全文化》，了解并每时每刻都能做到保护彼此的安全。

社交媒体的问题

虽然社交媒体平台对活动家和人权维护者来说有多种多样的用途，但其背后最常见的用途是分享信息、创建活动、协调和组织，以及参与讨论。

我们发布过 https://www.patreon.com/posts/wei-shi-yao-dong-42581802 。这是基于活动家的基本利益的考虑。所以，您需要一个基于您的具体工作的具体分析，每一项工作可能都是不同的，于是您应该掌握一套判断标准，而不是听从他人的指挥。

[image]

延伸：https://iyouport.substack.com/p/as45-

您的身份

如果您想保护自己的隐私，值得考虑使用集体身份。用假名与不同的人共享同一个账户可能是一种很好的方式来混淆算法，并在收集的关于您的数据中产生噪音。

每个人都有自己不同的模式和习惯，可以用来识别他们。让亲密团队中的所有人拥有相同的个人资料是混淆这些模式的好方法。

BACK [image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

行动者的成功永远不会是个人成功，对于行动者来说只有好的团体协作才能获得真正的成功。

与更多公众分享信息

如果您不得不使用寡头公司的社交媒体平台的原因是为了与更多的公众分享信息，请考虑以下几点：

您想让所有人都看到您的分享吗？如果不是，您可以使用朋友列表，如果您在Facebook上的话。列表允许您策划谁可以看到什么，但是，这并不能阻止 Facebook 访问和存储您的数据！

登录到 Facebook 帐户后您会发现 “朋友列表” 的左手栏下：

- 点击 “新闻源” 左侧的 “探索” 下的 “朋友列表”
- 单击 “创建列表”
- 为您的列表输入一个名称和您想添加的名字。您可以随时从列表中添加或删除联系人
- 单击 “创建”

给您的列表取名时要有创意。请避免用 “家庭” 来代表您的家庭成员，用 “工作” 来代表工作联系人；也要避免使用 Facebook 的 “智能列表”，它是基于从您的个人资料中收集的数据。分类包括您的家乡、居住城市、住址等。这些名单会暴露您的联系人，即使他们选择不与 Facebook 分享他们的信息。例如，如果您将某人添加到你所在城市的智能列表中，而这个人还没有将这些信息包含在他们的个人资

料中，Facebook 就会要求他们将城市添加到他们的个人资料中，并且也会将他们的个人资料放在该城市下。

从现在开始，当您发布一些东西时，您可以对谁能看到您的帖子有更多的控制。但是，要记住，如果您的列表上的任何一个人的账户或设备被泄露，您分享的内容也会被恶意者看到。使用社交媒体是一系列的权衡，您应该始终评估相应的利弊。

Facebook

有各种不同的选择来替代 Facebook，但当您建议使用这些替代平台时，您会听到的一个常见的说法是 “用户量太少了没有影响力”。但也并不是每个人在 Facebook 刚开始的时候都在 Facebook 上，邀请您关系网络内的联系人加入您的某个替代平台可能是值得的 —— 即使只是为了您正在做的敏感工作，同时维持一个 Facebook 账户用于个人事务。

如果您和亲密团队的成员忽然间消失在一个热门平台上，对监视者来说这就是一个 “信号”，你们反而会成为监视目标。所以安全原则上，我们会更多建议 分身 ，而不是彻底弃用和全面转移。具体解释见 [image]安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动

一般来说，重要的是要战略性地考虑您用什么工具来做什么。为各种任务使用不同的平台将有助于分散您的个人数据的危险性。

像 Diaspora 这样的平台是开源的，面向用户控制的。它们是分散化的，这意味着没有一家公司可以拥有您的数据或所有用户的数据。

推特/X

Twitter 的隐私设置比 Facebook 少得多，但在推特保护自己的隐私还是比较容易的。通过使用一个值得信赖的VPN，在创建账户和使用过程中谨慎对待自己分享的任何个人信息，以及避免与个人联系人分享

信息的对话。 https://iyouport.substack.com/p/as21-?s=w

但是，如果您是一个从事政治活动的个人或者是从事敏感工作的行动主义网络的一部分，监控可能是一个严重的威胁，特别是在风险国家。例如标签和使用标签的人很容易受到监视和社交图谱的影响。

对于从事敏感活动和关注政治的异议人士来说，请至少了解这些 [image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗 。

Twitter的替代选择

Mastodon 是与Diaspora遥相呼应的Twitter替代品。它是开源的、去中心化的，允许用户创建自己的 “社区”，前提是，您需要一个服务器。

[image]

可在本站“工具”专题中搜索“替代品”，以查找适合您需求的选择。

[image]

创建和宣传活动

许多人说他们在 Facebook 上了解活动，许多团体发现这个工具有助于组织聚会和邀请人们。许多人发现它是一个有用的方式来跟踪出席和与参与者分享更新。但是，Facebook 和可能访问您的活动的对手（比如警察）都可以收集所有这些数据。如果您正在策划一个敏感的活动，或者是一个可能吸引对手的政治集会，最好不要使用**Facebook**。

或者您还可以考虑使用仅限邀请的私人活动，确保标明只有主持人可以发出邀请。

[image]

作为替代，可以考虑使用传统的方式，如海报、电子邮件、传单和短信进行邀请。比如见这里《被压迫者的教育学，和”高级传单”》。

如果您是一个行动主义团体成员或活动家，经常为一个封闭的亲密团队或一个确定的网络组织活动，可以考虑花时间在Crabgrass上建立一个账户。Crabgrass 是一个安全的基于网络的组织工具，专门为活动家设计。它可以作为一个社交平台，在这里您可以与其他人讨论，也可以在私人团体中组织任务。这是一个专门为满足自下而上的草根组织需求而定制的社交网络工具，因为它能够在线协作，分享文件、任务和项目。

群组

许多基层团体和活动家网络利用 Facebook 群组进行讨论，汇集链接和信息，并组织即将举行的活动。当面对面会面不容易或不可能时，这尤其有帮助。但是，虽然 Facebook 群组可以 “关闭”，但问题还在于您是否愿意将您的数据和所有联系人分享的信息存储在一个监视资本家的服务器上。

为此，Crabgrass 是一个很好的选择。它允许 Facebook 群组允许您做的一切，并增加了一层隐私和安全性。

通信

Messenger 是最容易被取代的 Facebook 服务，因为存在各种安全、开源、加密和高效的替代品。与 Facbeook 提供的其他服务不同，Messenger 其实有多个值得竞争的替代品，您可以考虑 Signal、Riot 和Jitsi。

[image]
[image]

他们如何抓捕说真话的人？灾难和教训

[image] 关键词	吹哨 数字卫生 直接行动 自卫
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2021年7月4日
[image] **Description**	操作安全性

不论您是谁、做过或没做过什么，只要你的对手想要针对你，他们就会使用这些方法。任何政府间谍都可以使用这些手段，因为这些手段所基于的数字技术是全球共享的。

- Table of Contents

[image]

学校和真实生活之间的一个重要区别在于：学校先教你知识然后考试，生活则是先考试再教你知识。不需要亲自被考糊了才能学到东西，一直都有人被“考糊”，他们的教训应该成为更多人的知识。

我们必须重点推荐这篇报告，向更多人推荐；因为，这其中分析到的所有政府抓人和取证的手段，是任何政府都惯常使用的，而且，全球只有中国和美国能使用它们全部。

这是一系列血淋淋的教训。提醒读者特别注意本报告中含有的诸多超链接；它们就是所有人能否活在这个世界的基本功。

[image]

越来越多的人受到“间谍法”的政府指控，但是他们并不是什么“间谍”。

他们只是很普通的人，携带着自动备份到云端的智能手机；当他们想与某人交谈时，会给对方发短信或打电话；他们使用 Gmail 并在 Facebook 上分享 meme 和谈论政治；有时他们甚至从工作用的计算机登录这些帐户。

就像绝大多数人那样活着。

然后，他们在工作过程中看到了一些令人不安的事。也许是因为政府经常不知道无人机袭击杀死的人是否是平民；或者国家安全局在2016年目睹了针对地方选举官员的网络攻击，情报部门认为这是由俄罗斯精心策划的，尽管总统总是在电视上反驳；再或者，只是看到了 **FBI** 如何利用隐藏的漏洞渗透监视政治异议人士和宗教团体……

因此，这些普通人开始搜索政府数据库以获取更多信息，并可能打印出了他们找到的一些文档，真相和证据。

他们使用 Google 搜索了相关信息；也许他们甚至会向朋友发送短信，告诉他们在考虑可能的后续步骤时这是多么的疯狂……

他们应该联系记者吗？他们想要说出真相。

对真相的追求驱使他们开始查找自己喜欢的新闻机构的提示页面，并开始研究如何使用Tor浏览器。

所有这一切都发生在他们第一次联系记者之前。

目前为止大多数人仍不太了解监视，但可以肯定，我们所有人都是监视的受害者。电信公司和技术巨头几乎可以访问我们所有私人数据，从我们在任何特定时间的确切物理位置、到我们的短信和电子邮件的

所有内容。

即使私人数据没有直接发送给科技公司，我们的设备仍在本地保存了这些数据。你还记得两个月前的今天下午3:05，你在电脑上做了什么吗？你不记得了，但是你的网络浏览器会记得。

然而，虽然所有人都在受到广泛的监视，但是对于政府雇员和承包商来说 —— 特别是那些有安全许可的人 —— 隐私几乎是不存在的。

他们正是能说出巨大真相的人。因为他们有机会接触到真相。

每当他们搜索数据库时，他们使用的每一个搜索词和他们搜索的确切时间，都会被记录下来，并与他们的个人身份直接联系。

当他们访问一个秘密文件时，或者他们打印任何东西时，或者当他们将USB记忆棒插入他们的工作计算机时 …… 一切都被监视着，一切都被记录下来了。

可能存在员工截取屏幕截图或复制粘贴某些内容的确切日志。即使他们试图通过直接拍摄屏幕照片来绕过工作电脑监视，他们的工作场所无处不在的摄像机也可能记录他们的一举一动。

这就是透明度革命面前的那堵墙。

拥有安全许可的政府工作人员需要承诺 “绝不向任何未经授权接收的人透露任何机密信息”。

但是，对于许多透明度革命的支持者而言，公开这些秘密的决定源于对政府阴谋的疑虑，同时深刻的认识到，只要该阴谋保持机密，这个体制就不会改变。

虽然对于在内部提出问题或向国会提出申诉的举报人提出了一些保护措施，但是，这些人仍然会因说真话而受到惩罚，这一惩罚的历史是

很悠久的。

所谓的“间谍法”正在被越来越多地使用。这是一项1917年颁布的法律，规定：如果“有意或有理由相信该信息将被用于对美国的伤害或给外国人的利益”，那么公开该信息的任何人都会违反“间谍法”。

该法律本身充分体现了体制针对说出真相的人的打压。

根据该法律规定，政府内部人士不得辩称，他们决定分享这些信息的决定是出于帮助广大公民对抗和结束被政府虐待之厄运的热情。

“该法案对公众有兴趣了解政府的无能、腐败或犯罪的可能性视而不见，政府保护特定秘密的政治利益被置于超越一切的位置上”，第一修正研究所所长 Jameel Jaffer 最近写道。

在特朗普时代涉嫌泄密的四起所谓的间谍法案件中，最不寻常的关注就是：前中央情报局软件开发商 Joshua Schulte，他被指控泄漏 CIA 文件和黑客工具，也就是WL公开的著名 Vault 7 披露。

Schulte 的案例与其他案件有所不同，因为在FBI于2017年3月扫荡他的家并没收了他的台式电脑、电话和其他设备之后，政府使用所谓的儿童色情来诽谤他（显然当局的扫荡并没有拿到泄密证据）。

检察官最初对 Schulte 提出了多项与儿童色情制品有关的罪名，后来又在另一起案件中受到所谓的性侵犯指控。

直到2018年6月，政府才最终根据所谓的“间谍法”指控他泄漏黑客工具。他对所有指控都表示不认罪。其他三起因涉嫌泄露政府机密的所谓“间谍法”案件，均涉及被认为是独立媒体 Intercept 的消息来源。

intercept 是为了专门发布斯诺登文件而创立的出版物，此后一直在公开披露符合公共利益的各种来源的秘密政府文件，也一直是特朗普政府对透明度革命的战争中具有吸引力的目标，这并不奇怪。

BACK https://iyouport.substack.com/p/lr--6f2?

utm_source=publication-search

政府参与这场战争，如“间谍法”这样的法律已经很成熟，可以各种滥用，并且拥有压倒性的监视技术火力，当应用于政府自己的工作人员和承包商时，几乎没有任何限制。

但记者也可以使用各种工具来抵御，包括第一修正案，并提供教育，普及政府用来跟踪和监视的各种方法，以学习反监视反侦察的能力。

Intercept 已经对特朗普政府司法部提交的所有七起泄密案件中的法院文件进行了审查，以确定了政府用来抓捕说真话者的方法。

这些政权常用的抓捕方法对于反侦察的行动者来说至关重要。

[image]

当透明度革命萌芽于政府部门内部时，联邦调查局可以获取大量的数据 —— 这些数据准确描述了政府计算机上发生的一切事、以及谁在政府数据库中搜索了什么，这有助于缩小嫌疑人名单。

有多少人访问过这个文件？多少人打印过它？他们的任何工作电子邮件都可以用来起诉他们吗？可以从他们的工作计算机中提取哪些证据？

一旦FBI根据政府自己收集的大量数据列出了嫌疑人名单，他们就会使用法院命令和搜查令来获取有关其调查目标的更多信息。

他们迫使技术公司（这些公司的商业模式通常依赖于收集尽可能多的用户信息）来交付所有内容，包括个人电子邮件、短信、电话元数据、智能手机数据备份、位置数据、存储在 **Dropbox** 中的文件等等 …… 以及更多。

联邦调查局特工袭击了说真话的人的家、搜查了这些人的车子，从他们找到的任何手机、电脑和硬盘驱动器中提取任何东西。

有时，还包括说真话的人认为自己已经删除了的文件（实际上并没有彻底删除）、或通过 **Signal** 或 **WhatsApp** 等加密消息服务发送的文本消息和文档。

这些应用程序使用的加密技术可以使消息在通过互联网传输的过程中受到保护，这些服务本身也无法监视内容或将其移交给政府，但是，如果手机和电子设备被当局抢走，任何加密都会失败。

这就是 Facebook 琢磨出来的能打死一切加密的方法 —— 瞄准设备本身，BACK https://web.archive.org/web/20200927061918/https://www.iyouport.org/facebook-%E7%BB%99%E4%BA%86%E5%85%A8%E7%90%83%E5%BD%93%E6%9D%83%E8%80%85%E4%B8%80%E4%B8%AA%E7%BB%88%E6%9E%81%E6%9A%B4%E6%94%BF%E8%93%9D%E5%9B%BE/

由于这些说真话的人真的不是间谍，所以他们通常不知道该如何避免这种监视……

前中央情报局和国家安全局承包商 Edward Snowden 是最了解政府监视能力的人，就连他也并没有找到任何方式能够在将政府秘密公之于众的同时保留自己的匿名性。

“我感谢你对我的安全的关注”，斯诺登在一封加密的电子邮件中写道，这封邮件是通过匿名地址发送的，使用的是 Tor 网络，在2013 年春天写给电影制片人 Laura Poitras，信中写道：“我已经知道这将如何结束，我接受风险。”

在纪录片“第四公民”中，斯诺登解释说，他在接触记者时采取的安全措施只是为了给自己足够的时间来获取有关美国国家安全局对全球公众的大量侵犯隐私的证据。

“只要时间充裕，当局能找到一切。我不认为有任何方法能保持我的安全匿名，”他在香港的一个酒店房间里说，然后他决定主动公开自己的身份。

> 如果我们想要生活在一个所有人在看到不公时都能大声说出来的世界里，我们就需要那种能够保护每个人隐私的技术，并且需要默认启用它。

要让人们有机会说出真相，让说出真相的人也能平安地活下去。

[image]

2017年在特朗普成为总统后，他的司法部发出了第一份针对透明度革命勇士的起诉书，其中司法部根据“间谍法案”指控 Reality Leigh Winner 将一份绝密的国家安全局文件泄露给了新闻机构 The Intercept。

当时，Winner 是一位25岁的美国空军退伍军人，也是一位专注于缓解气候危机的 CrossFit 教练。

根据法庭文件，Winner 是仅有的六个能接触到该机密文件的人之一，她打印了她被指控泄露的文件（法庭显示她于2017年5月9日进行了搜索、访问并打印了该文件）。

在搜查了所有六名员工的工作计算机后，当局发现 Winner 是唯一一个与发布该文档的新闻机构有电子邮件联系的人。（她使用的是私人 Gmail 帐户，足见有多么不安全）

联邦调查局特工随后搜查了她的家，并在没有律师在场的情况下对她进行了讯问，并没有告知她有权保持沉默，侵犯了她的米兰达权利。

在她家里，当局的特工找到了关于如何使用一次性电话号码和 Tor 浏览器的手写笔记。（可怜的人，她真的对保密技术一无所知）

当局还抢走了她的 Android 智能手机和她的笔记本电脑，从两台设备中提取了证据。

联邦调查局还命令多家科技巨头公司从 Winner 的账户中提取信息。

Facebook 提供了 **Winner** 的 **Facebook** 和 **Instagram** 帐户的数据，谷歌提供了 **Winner** 使用的两个独立 **Gmail** 帐户的数据，**Twitter** 提供了 **Winner** 帐户的数据，**AT＆T** 也在此做出了“贡献”。

并不确切知道这些公司都提供了多少数据，但可以知道他们被要求披露与 **Winner** 账户相关的所有信息，包括：

- 用户名，电子邮件地址，实际地址，电话号码和信用卡号；
- 每次登录时的历史记录，持续时间以及IP地址；
- 还有关于这些服务所涉及的每个通信实例的元数据，包括通信类型、来源和目的地，以及通信的文件大小、持续时间。

FBI 还要求与 Winner 的 Facebook、Instagram、Google、Twitter 和 AT＆T 帐户相关联的所有记录 —— 请注意这是使用相同的电子邮件地址创建的帐户、从同一 **IP** 地址访问、或从同一 **Web** 浏览器登录的帐户。

此处强调了 分身 对于安全的重要性。

如果用户没能采取额外步骤保持匿名，则服务提供商可以轻松链接从同一台计算机访问的不同帐户。

FBI 还从 **Winner** 的手机中提取了所有内容：

- 她的照片，包括 2017 年2月7日拍摄的一张网页照片，其中列出了由不同媒体机构运营的八台 SecureDrop 服务器。
- 从她的智能手机应用程序中提取的数据，例如 Facebook 应用程序，其中包含她与姐姐交换的私人消息，这些私人信息后来都被用于针对她的打击。

- 她的手机浏览器历史记录：3月7日，她访问了一个网站，其中包含“暗网电子邮件提供商”列表，并在谷歌上搜索了“tor email”关键字。

- 5月9日，“大约下午7:29:49（美东时间）”，Winner 搜索并查看了她被指控泄露的 NSA 文件的新闻媒体的页面，以及第二个新闻媒体的页面; 那天晚上，她登录了她的 Dropbox 帐户，三分钟后，她再次查看了第一个媒体组织的页面。

这就是我们在“完美隐身”系列中强调的：如果您不能熟练使用全套匿名技术，切勿使用互联网搜索任何有关自己的东西。

因此 FBI 获得了发给 Dropbox 的搜查令，要求交出存储在 Winner 帐户中的所有文件和其他信息，以及 —— 请注意！“任何已经被本人删除但仍可供 **Dropbox** 公司使用的消息、记录、文件、日志或信息” —— **Dropbox** 给了 **FBI** 一个包含所有这些数据的拇指驱动器。

FBI 还获得了向 Google 发出的搜查令，要求几乎所有存储在 Winner 帐户中的内容，包括：

- Gmail 帐户中的所有邮件 —— 不要使用Gmail， [image]隐私自助：流行产品的开源替代品目录

- 她的全部谷歌搜索历史记录 —— 所谓的“隐身模式”是骗局，根本不会保护你，你需要做的是：Tor [image]一句话安全须知：记住这些句子，以简单地优化您的安全性

- 她的位置历史记录 —— 即使关闭了“位置历史记录”设置，谷歌仍然可以记录你的位置；

- 可以基于Web浏览器 cookie 识别的所有活动（这可能包括她访问过的使用 Google Analytics 服务的任何网页的列表）

- 还有她的安卓手机备份， [image]如何保持 Android 设备免

受警察的侵害

FBI 获悉了一个新的、单独的谷歌帐户，他们怀疑是 Winner 使用的，这是以前没有人知道的账户。搜查令也要求提供该帐户的其他数据。

谷歌向 FBI 提供了关于 Winner 的两个谷歌账户的全部数据，超过 **809mb**（压缩后）。

FBI 还从 Winner 的笔记本电脑中直接提取数据。当局发现她在2017年2月1日下载了 Tor 浏览器，并在2月和3月使用过它 —— 请注意使用 **Tor** 浏览器并不违法！但是，有可能在当局眼中是“重大”嫌疑，对于举报人 **Joshua Schulte** 当局能拿出的唯一“证据”就是他使用了 **Tor**。

所以，有经验的人应该注意保持所有电子设备的*干净*，也就是定期做大清洗；此外，切勿在行动之前才下载使用这些安全工具，它们应该是您日常的上网习惯，而不是应急灯。 BACK **[image]** 大清洗 - 扫荡危险区域：完美隐身 **S04E07**

FBI 还发现了一个保存在她桌面上的note，其中包含一个名为 VFEmail 的小型电子邮件公司的用户名和密码，因此，这些政府特工还获得了另一个搜索令，要求提供 VFEmail 帐户中所有内容的副本。

此处提醒：尽可能用纸笔记录重要内容是对的，但是，必须及时销毁所有记录 —— 烧掉它们，不要简单地手撕或者粗糙的碎纸机。

Winner 被判有罪，并被判处五年有期徒刑，这是联邦法院对新闻爆料人判处的最长刑期。

[image]

根据法庭文件，在 Terry Albury 在联邦调查局长达16年的反恐职业生涯期间，他“经常在单位内部观察到或经历过种族歧视和偏见”。

作为明尼阿波利斯办事处唯一一位黑人联邦调查局特工，他对该局内部的“系统性偏见”感到特别不安，特别是在联邦调查局虐待线人时。

2018年，司法部对 Albury 提起了所谓的“间谍活动”诉讼，声称他向一家新闻机构泄露秘密文件。

据报道，The Intercept 于2017年初发布了一系列基于FBI内部机密的披露，其中包括有关该情报机构秘密调查少数民族公民、和监视记者的诸多恶劣行为，其证据被认为来自 Terry Albury。

尽管联邦调查局不知道文件是否在分享之前已经被打印过，但是要跟踪是谁访问过这些文件，并不难。

联邦调查局确定了有16人访问过媒体组织在其网站上发布的27份文件之一。

当局搜查了所有这些人使用的16台工作电脑，包括 Albury 的电脑，并发现他也获得了“超过三分之二”的公开文件。

根据法庭文件，FBI 把从 Albury 的计算机上挖到的各种活动都作为对他指控的证据：他访问了哪些文件以及何时访问的、何时拍摄了屏幕截图、何时将这些屏幕截图复制并粘贴到文档中、以及何时打印出来……

例如，数据显示，2016年5月10日下午12:34 ~ 下午12:50之间，Albury 访问了两份机密文件。

记录还显示，十九分钟后，他将两张截图粘贴到未保存的 Microsoft Word 文档中，在接下来的45分钟内，他将11个截图陆续粘贴到未保存的 Excel 文档中。

一整天，他访问了更多政府秘密文档，将更多屏幕截图粘贴到 Excel 文档中。

在下午**5：29**，他把所有这些打印了出来，然后关闭了文件而不保存。

并且，不仅仅是他的工作计算机受到了监视；**FBI** 通过在他工作场所安装的诸多闭路视频监控系统，拍摄到了 **Albury** 的视频。

在2017年6月16日、8月23日和8月24日，监视系统记录了 Albury 拿着银色的数码相机，插入了“看似数字记忆棒的东西”，并拍摄了他的屏幕照片。

法院文件说，在这三天里，Albury 都在他的电脑屏幕上查看文件。

“（FBI 使用的虐待和间谍行为）这是人权问题”，法庭文件显示 Albury 的妻子要求轻判。

40岁的 Albury 认罪了，被判处四年监禁和三年监外察看。

[image]

像 Signal 和 WhatsApp 这样的通信服务，理论上可以使记者能够通过端对端加密技术安全地与他们的消息来源进行通信，这样只有对话双方的电话才能访问信息，服务本身也无法访问。

当使用 Skype 和 Slack 等非加密消息传递服务、Twitter 和 Facebook 上的直接私信服务、或普通文本短信和电话时，非常不安全。

但是，当手机遭遇物理搜查、并且用户尚未删除其消息历史记录时，加密服务不会保护你。

这在2018年6月7日已经非常清楚了，当时司法部起诉前参议院情报委员会助理 James Wolfe 向 FBI 作出虚假陈述。

根据法庭文件，Wolfe 告诉联邦调查局，他没有与记者联系过。

但是对 Wolfe 的起诉中引用了他与记者通过加密通信 **Signal** 进行对话的内容。

起诉书没有提到 FBI 是如何获得这些加密消息的，但唯一合理的结论是，间谍在搜查他的电话时发现了这些消息。

除获得他的 Signal 消息之外，FBI 还搜索了 Wolfe 的工作电子邮件，并找到了他与记者通信的消息。

由此，联邦调查局知道了他与记者的会面、以及会面发生的地点。

当局挖到了 Wolfe 与记者交换过的数百条短信、与他交谈的记者是谁、以及发生在什么时间。

在同一调查期间，司法部向谷歌和 Verizon 发出法院命令，要求查获属于纽约时报国家安全记者 Ali Watkins 的多年来的电话和电子邮件记录，后者之前曾为 BuzzFeed News 和 Politico 工作过。

联邦调查局正在调查 Watkins 的一篇 BuzzFeed 文章的消息来源，该文章的内容是关于一名俄罗斯间谍试图招募特朗普顾问卡特佩奇。

被查获的记录甚至一直追溯到 Watkins 的大学时光。这是特朗普政府打击记者所做的第一例案件。

Wolfe 承认向调查人员说谎关于与媒体有联系，并因此被判处两个月监禁、和7,500美元的罚款。

[image]

即使没有物理搜查电话，**FBI** 也可以获取实时元数据，该元数据显示是谁向谁发送了消息，以及何时发送的，通过至少一个加密的消息传递应用程序。

这种情况发生在 Natalie Mayflower Sours Edwards 身上，她是财政

部金融犯罪执法网络（FinCEN）的高级官员。

在2018年底，司法部起诉 Edwards 涉嫌将机密消息提供给了一名记者，据报道这名记者是 BuzzFeed News 的 Jason Leopold，详细介绍了涉及共和党成员的可疑金融交易、特朗普竞选团队的高级成员，以及与克里姆林宫有联系的俄罗斯特工和俄罗斯寡头。

根据法庭文件，**FBI** 为 **Edwards** 的私人手机获得了“被授权的”监视跟踪。

这是一项法院命令，允许 FBI 使用一系列技术从手机收集各种类型的通信元数据 —— 例如，命令第三方移交此元数据、甚至可以使用 **[image]** 黄貂鱼 欺骗手机连接。

使用此法院命令，FBI 显然能够从 Edwards 手机上的加密消息应用程序中收集到实时的元数据。

例如元数据记录显示，在2018年8月1日上午12:33，上述法院命令“开始生效”后的6小时、以及 BuzzFeed News 发布其中一篇报道后的第二天，Edwards 据称与记者交换了**70**条加密消息。

第二天，在BuzzFeed News发布另一报道的前一周，Edwards 据称与记者交换了**541**条加密信息。

法庭文件中没有写明 FBI 监视的消息传递应用程序是哪个，并且不清楚政府如何获得的元数据。

Signal 的创始人 Moxie Marlinspike 表示，他的应用程序对此不负责。

“Signal 被设计为保护隐私，并尽可能少地收集信息，” Marlinspike 告诉 The Intercept。

“除了每条消息的端到端加密外，所有用户的联系人、他们所在的群组、任何群组的标题或头像、甚至用户的个人资料名称或头像的任何记录，Signal 都不读取”；“甚至GIF搜索都受到保护。大多数时候，Signal 的新 Sealed Sender 技术意味着我们甚至不知道谁是消息传递者。连第三方数据我们都几乎无法提供”。

WhatsApp 的一位发言人表示，他们不能对个别案件发表评论，并指出其有关回应执法要求的常见问题部分。

该文件指出 **WhatsApp** “可以收集、使用、保存和共享用户信息，如果我们真诚地相信”有必要“”回应执法程序或政府要求的话”。

显然，WhatsApp 很不安全。

请注意，根据 Facebook 的透明度报告，其中包括对 WhatsApp 用户数据的请求，在2018年下半年，当针对 Edwards 手机的监视开始运作时，Facebook 收到了4,904个“Pen Register / Trap & Trace”请求的回应，其中要求提供的数据波及 **6,193** 位用户，并且，**Facebook** 回复了其中**92**%的数据请求。

这就是为什么使用 Facebook 以及属于该公司的所有应用都非常危险 —— 并不在于您本人“做了什么”，您的所有联系人（包括联系人的联系人）中如果有任何一个人被当局怀疑，都会波及到您。

Apple 在此也一样。

Apple 发言人拒绝发表评论，但和 Facebook 一样引用了其法律程序指南中有关 Apple 可以向执法部门提供的与 **iMessage** 相关的数据类型的部分。

该指南称：“iMessage 通信是端到端加密的，Apple 在设备之间传输时无法解密 iMessage 数据，Apple 无法拦截 iMessage 通信，Apple 也没有 iMessage 通信日志。”

但是，**Apple** 确实拥有 **“iMessage** 性能查询日志”，这足够表明一个用户的 **Apple** 设备上的应用程序已开始向另一个用户的 **iMessage** 帐户发送消息。

该指南写道：“iMessage 性能查询日志最多可保留30天；并可以通过 18 U.S.C. §2703(d) 或具有同等法律标准的法院命令或搜查令获得。”

联邦调查局还命令 Edwards 的个人手机运营商交出她的电话记录；FBI 还对她的一位同事做了同样的事，后者被称为“同谋”。

联邦调查局获得了 Edwards 的个人电子邮件帐户搜查令（大部分可能是 Gmail），并从中获取了她的“互联网搜索历史”记录 —— 她被指控在文章发布后搜索了所谓的泄漏消息相关的多篇文章。

联邦调查局获得了搜查令以实际搜查她的全部，并查获了一个USB闪存驱动器，以及她的个人手机。

根据刑事诉讼，该闪存驱动器中包含24,000个文件，包括数千个描述政府可疑金融交易的文件。

FBI 还从 Edwards 的电话中直接提取了消息应用程序数据，也就是说，这些间谍可以直接阅读她据称与记者交换的消息内容。

Edwards 面临长达**10**年的监禁。她已经拒绝认罪。

[image]

政府工作人员通常能够使用他们登录和搜索的内部数据库访问受限的文件，包括由国防承包商 Palantir 等私营公司运营的数据库。

这些数据库跟踪每个用户的行为：他们搜索的术语、他们点击的文间、他们下载到计算机的文件……

美国国税局官员 John Fry 可以访问多个执法数据库，包括 Palantir

运营的数据库，以及 FinCEN 的数据库 —— 后者就是 Edwards 被指控泄漏可疑活动报告所在的数据库。

今年2月，司法部起诉 Fry 据称提供了有关涉及特朗普前律师 Michael Cohen 与著名律师 Michael Avenatti 的可疑金融交易的详细信息，还有至少一名记者、纽约客的 Ronan Farrow。

在其中一次交易中，也就是在2016年大选前不久，Cohen 向一位成年电影女演员支付了130,000美元的封口费，以换取她所说的与特朗普的婚外情故事保持沉默。

据法庭文件显示，在2018年5月4日下午2:54，国税局官员 Fry 据称在 Palantir 数据库中搜索了与 Cohen 有关的信息，并下载了5份可疑活动报告。

同一天，Fry 据称对 FinCEN 数据库中的特定文件进行了多次搜索。

FBI从他的个人手机运营商那里获得了 Fry 的电话记录。在下载了与 Cohen 有关的可疑活动报告后，Fry 据称打电话给那位著名律师 Avenatti。

这些监视数据还显示，此后他又打电话给记者，并通话42分钟。

FBI 随后获得了 Fry 手机的搜查令。据报道，在2018年5月12日至6月8日期间，Fry 与记者交换了**57条 WhatsApp** 消息。

监视数据显示，该报道发表后，他发了一条短信，其中写道，“写得非常好”。记者的手机号码据称就在 **Fry** 的手机联系人名单中。

黑体字是严重的教训！

Fry 面对五年的监禁。他拒绝认罪。

[image]

Daniel Hale 2009年加入军队之前在意识形态上一直反对战争，当时他21岁，但他觉得他别无选择。

“我无家可归，我很绝望，我无处可去。对于我来说这是最后一站了，空军准备接受我，“ 他在 “National Bird“ 中说道，这是一部关于曝光无人机作战内幕的举报人的纪录片，**2016** 年出版。

在接下来的五年里，Hale 一直在为国家安全局阿富汗联合特种作战特遣部队的无人机计划工作，并作为国家地理空间情报局的国防承包商。他的工作包括帮助确定被暗杀的目标。

Hale 也是一个直言不讳的活动家。

“我参与无人机行动的最令人不安的事就是，我担心自己参与杀戮或捕获的任何人中包括平民，这是不确定的，” 他在那部纪录片中说，“没有办法知道。”

今年5月，司法部指控 Hale 因涉嫌泄漏与无人机战争有关的机密文件、并向特朗普政府官员确认为 The Intercept 的新闻机构提供了信息，被视为进行“间谍活动”；Intercept 于2015年发布了一系列有关该事件的最详细报道 —— 美国政府的暗杀计划。

“在5月9日开封的起诉书中，政府声称美国无人机计划的文件被泄露给了新闻机构”，Intercept 总编辑 Betsy Reed 在关于 Hale 起诉的声明中表示。

“这些文件详细说明了政府如何通过无人机袭击瞄准和杀害世界各地的人民，包括美国公民，一切秘密的和不负责任的程序。这些信息具有至关重要的公共利益，与其披露相关的活动理应受到第一修正案的保护。

“但是，但是！说出真相的人面临长达**50**年的监禁！而在这些无人机杀戮中，没有任何人因杀害平民而被追究责任 **……**

2014年8月8日，数十名联邦调查局特工突袭了 Hale 的家，手持枪支，搜查了他的电脑和闪存盘。

这一切都发生在奥巴马政府期间，当时奥巴马政府拒绝提出指控。但是五年后，特朗普政府的司法部重新审理此案。

根据法庭文件，政府间谍可以看到 **Hale** 据称在他使用的不同计算机中输入的确切搜索词，一个用于非机密工作，另一个用于机密工作，以及何时进行的任何搜索。

用来攻击他的所谓证据包括 Hale 据称发给他的朋友的短信，以及他据称与媒体机构已经确定为 The Intercept 的记者 Jeremy Scahill 进行的文本和电子邮件对话。

当局描述了 Hale 的电话元数据。当局声称 Hale 参加了书店的一个活动，就坐在记者旁边。所有这些事都发生在 Hale 据称向媒体发送任何文件之前。

根据起诉书，在2013年9月至2014年2月期间，Hale 和记者 “通过 Jabber 进行了至少三次加密通话”，这是一种在线聊天服务。

目前还不清楚政府在哪里获得的这些信息；可能是来自大规模的互联网监控、Jabber 聊天服务提供商、或者直接是对 Hale 的计算机进行的物理分析。

正如 Winner 和 Albury 的情况一样，FBI 确切地知道 Hale 打印了哪些文件以及何时打印的。

据称，Hale 打印了32份文件，其中至少17份后来被新闻机构“全部或部分”发布。

当联邦调查局袭击 Hale 的居所时，据称特工在他的计算机上发现了一份未分类的文件，以及一份 **Hale “试图删除”的USB**记录文件。

当局还发现了另一个包含 **Tails** 的 **USB** 记忆棒，这是一个旨在保持数据和互联网活动私密和匿名的操作系统，可以通过USB记忆棒启动，尽管 FBI 似乎没有从中收集任何数据。

政府间谍在 Hale 的手机联系人薄中找到了记者的电话号码。

现年32岁的 Hale 面临最高**50**年的监禁。他已经拒绝认罪。

[image]

想要说真话，并不容易。不同的人面临着截然不同的风险。

如果您在 Google、Facebook 或 Goldman Sachs 等公司工作，您的工作设备可能会受到严格审查，但您的个人设备仍然无法直接被雇主的监控（只要您不依赖这些寡头公司控制的任何服务与记者沟通）。

一些政府内部消息来源可能有办法访问秘密文件，其披露符合公共利益，不涉及生成带有时间戳的日志条目不会将其用户名与该访问权限相关联。

越来越清楚的是，用于起诉举报人的主要证据来自于他们与媒体联系之前发生的事，甚至在他们决定行动之前发生的事。

但是，记者做出充分准备尽可能保护他们的消息来源仍然是至关重要的，如果说真话的人请求帮助，记者应该尽力而为。

这包括运行像 **SecureDrop** 这样的系统，它为说真话的人提供了安全的和无元数据的通信方式，并最大限度地减少了设备上残留的联系人痕迹。

记者还应采取措施，通过始终使用加密的消息应用程序、而不是不安全的短信，并始终使用阅后即焚功能，以减少科技公司可以访问的信息量。

记者还应鼓励消息来源不要将记者的联系方式添加到手机联系人薄中，因为这些联系人薄可能会被同步到 **Google** 或 **Apple** 的服务器。

验证文件真实性的新闻过程 —— 也就是开源情报分析工程 —— 也会给匿名来源带来风险，但是，这一过程对于确定材料有没有被伪造或改变、以及保持可信度，至关重要。

但是，美国规定记者在发布报道*之前*需要主动拿给政府相关部门审查，以确定哪些内容政府愿意或不愿意公开。

这个过程不仅将杀死几乎所有真相的披露，并且，会令说真话的人和记者，都陷入严重的危险。

新闻机构还需要就发布内容做出艰难的决定。

有时，如果可以通过描述文档的内容来报道、并且可以掩盖消息来源时，媒体可能会决定不发布原始文档，这样更安全。

然而，这些方法虽然能保护消息来源，但也同时降低了对读者的透明度，也限制了报道的影响力，这对记者和举报人来说都很重要。

在所谓的“假新闻”标签被用来诋毁任何严肃的调查性新闻的时代里，只有原始的文件可以作为反驳这些指控的有力证据。

[image]

加密消息应用在保证在线对话方面取得了重大进展，但是，在保护消息来源方面仍存在重大问题。

其中许多这类应用程序，包括 WhatsApp 和 Signal，都鼓励用户将他们发送消息的联系人的电话号码添加到联系人列表中；但这些数据通常都会同步到云端，**WhatsApp** 甚至鼓励用户将他们通信历史记录备份到云端。

这非常危险。尽管拥有 WhatsApp 的 Facebook 无法访问这些备份消息的内容，但谷歌和苹果仍然可以访问。

端到端加密只能保护消息从一部电话传输到另一部电话的过程，但是，通信各方的每部电话仍然拥有所有这些消息的纯文本副本，这使得它们很容易受到当局物理搜查的攻击。

阅后即焚是一个很好的开始，但它们仍然需要进行改进。

用户应该可以选择自动让所有聊天记录消失，而不必记住每次开始对话时设置消失的消息，并且应该询问用户是否需要在首次设置应用时启用此消息。

尤其是，当对话中的所有消息都消失时，与该人进行对话的所有取证跟踪也应该消失。

同样，在保护元数据方面也还有许多工作要做。

Signal 的“sealed sender”功能可以加密 Signal 服务可访问的大部分元数据，比任何其他流行的消息传递应用程序都要强大，但它仍然不完美。

消息传递应用程序需要重新设计其服务，以便他们无法访问有关其用户的任何元数据，包括IP地址。

只有当消息服务本身也无法访问任何元数据时，才能保证数据不会泄漏给FBI 这类间谍组织。

默认情况下，Web 浏览器会保留您访问过的每个网页的详细历史记录。

这就是监视资本主义的盈利模式。他们不会在此做出任何改变 ——这就是为什么每个人都应该自己保护好自己。

本报告中的几乎所有超链接都应该给您带来帮助。

目前，Tor浏览器是保护用户隐私的最佳选择。只要操作方面不要出错 —— 人始终是最大的 bugs，而非技术。

但是，不幸的是，仅仅在计算机上安装 Tor 浏览器或其他隐私专用工具，就可以作为所谓的证据攻击说真话的人。

这就是 Mozilla 计划将 Tor 直接集成到 Firefox 中作为“超级私密浏览”模式的原因之一。

将来，希望说真话的人可以简单地直接使用 **Firefox** 内置的功能来获得相同级别的保护，而不是去下载 **Tor** 浏览器。

最后，Gmail、Microsoft Outlook、Google Drive、iCloud、Facebook 和 Dropbox ……等等这些大厂的服务彻底不应该使用。

再次强调：这是血淋淋的教训！本报告中涉及的几乎所有超链接都应该是警报器 —— 因为中国当局也是使用这些方法抓捕任何他们想要的人的。已经有太多人因此被扔进了监狱。

说出真相是有史以来最重要的反霸权斗争 —— 每一位加入这场战斗的人都应该获得最充分的保护。

我们要所有人都活着；活着享受你们亲手争取到的自由。

[image]
[image]

某个VPN可能不可靠的5个标志：如果您不理解技术的话

[image] 关键词	VPN 自检
[image] 关联	[image]如何检查您的VPN连接是否实际加密 ；[image]一句话安全须知：记住这些句子，以简单地优化您的安全性 ；[image]与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧
[image] 创建时间	2021年7月22日
[image] **Description**	操作安全性

VPN是一个每年价值数十亿美元的大生意。有了这么多钱，许多VPN供应商不值得信任也就不足为奇了。

- Table of Contents

  1、评论和建议
  2、介绍
  3、语言错误
  4、警惕免费
  5、检查记录
  6、不良政策
  做出正确的决定

[image]

这里的VPN指的是加密您的流量，以保护您不受ISP和政府监视的工具，而不仅仅是翻墙工具；能翻墙的VPN不一定安全，安全的VPN不

一定能翻墙。

如今，由于大规模监视的恐慌，VPN是一个每年价值数十亿美元的大生意。有了这么多钱，许多VPN供应商不值得信任也就不足为奇了。那么，您如何选择一个好的、值得信赖的VPN？尤其是在您可能不理解技术的情况下。

以下是您在打开钱包前需要注意的一些迹象。

1、评论和建议

要想知道一个VPN是否值得您花时间和金钱，一个公认的方法是通过互联网评论或您信任的人的推荐。然而，并不是所有的推荐技术的网站都同样值得信赖，因为其中一些可能是被开发商付了钱的“软广”。也不是所有朋友都能在此靠谱，您需要考虑的是朋友的技术能力，而不是他们有多爱您。

因此，建议您在查阅评论时谨慎行事，并注意几件事：首先，许多评论会转述营销文案，所以当您看到一个VPN供应商的网站和评论之间有太多的相似之处时，您可以认为这里面也许有一些猫腻。此外，如果评论中的说法听起来好得不像真的，或者语气似乎太“推销”，那么也最好不要信。

2、介绍

在购买VPN时，您应该注意的另一件事是服务的展示方式。虽然许多供应商—— 从NordVPN和ExpressVPN 这样的市场领导者开始——都习惯于对VPN的私密性进行略微夸张的宣称，但有些供应商则超越了这一点，然后再进一步。

这方面的一个例子是 X-VPN，它在其网站上声称有5000万用户。然而，快速浏览一下谷歌应用商店的下载页面就会发现，它被安装了超过1000万次。非常值得怀疑X-VPN真的有这么多用户吗？VPN是相当

受欢迎的应用程序，但它们的需求量并不大。

这只是一种夸张的营销方式，但有些服务比这种还要进一步，使用赤裸裸的恐吓手段来让您注册。这方面的一个例子是RusVPN，它打出了几个红旗。首先是一个名为 Brian 的美国人写的非常奇怪的推荐。这不是真正的人说话的方式：

[image]

当然，推荐语是现代互联网的组成部分，但进一步滚动，您会看到：

[image]

在这个的案例中，上图中描述的情况是假的，因为实际上我使用的是另一个代理连接到日本服务器，它没有意识到。

至于右边那个有威胁性的黑色块中的字，其中大多数信息（如银行账户和信用卡信息）都是通过使用HTTPS的连接来传输的，密码在发送前是经过散列的（不可读）。开启VPN并不会使这些信息的发送更加安全。

使用VPN有很多理由，但 RusVPN 声称如果你不使用VPN，你的密码和信用卡号码就会被抢走，这是公然的虚假广告。可悲的是，有很多其他供应商也在做同样的事。

3、语言错误

一个服务可能不靠谱的另一个小标志是语言使用不当。虽然不是每个人都会说英语，但在网站上有很多可见的拼写或语法问题是一个明显的迹象，表明有关的服务不是太热衷于细节。

一个专业的公司将为其网站配备专业的编辑人员。由于在运行VPN时，细节是相当重要的，这是一个红旗，尽管是一个小红旗。

4、警惕免费

另一个巨大的广告伎俩是提供免费的VPN服务。一般来说，人们已经知道不应该使用大多数免费的VPN。它们中有太多已经被发现向第三方出售数据，而一些不知名的VPN供应商也在做同样的事，这种风险实在太大了。隐私安全很重要，不能拿它做赌注。

但有一些像样的VPN服务在提供常规服务的同时还提供免费计划，通常是让您在决定付费之前对服务有一定的了解。其中最好的是 Windscribe 和 TunnelBear，它们都提供有限的免费服务，并且没有不良行为记录（请注意，这不是翻墙VPN）。

5、检查记录

说到这一点，在签署一项服务之前，您可能想做的一件事是对其名称进行网络搜索，也许甚至可以添加额外的关键词，如 “声誉”、“漏洞” 或 “出售数据”。虽然过去的表现并不总是判断一项服务现在如何的准确方式，但它可以给您一个指示，让您知道该公司是什么样的。

将其防病毒解决方案与VPN捆绑的 Avast 公司最近被发现通过其子公司 Jumpshot 出售用户数据。以色列的免费 VPN Hola 可能会劫持你的电脑加入僵尸网络，而且往往不会有特别好的启动效果。

当然，有些公司从其不光彩的过去中恢复过来了。几年前，IPVanish 犯了一些错误，PureVPN 也是如此，但这两家供应商似乎都从错误中吸取了教训，重新制定了他们的隐私政策，修复了任何需要修复的问题。虽然他们的历史可能使他们得不到令人振奋的推荐。

6、不良政策

在做出购买决定之前，最后一件事是您所关注的VPN的隐私政策。虽然您不能总是依赖销售商所说的内容（您可能不应该信赖任何应用程

序的隐私政策宣称 https://iyouport.substack.com/p/--e4f ）——但这是检查一项服务是否注意细节的好方法。

首先，您要确保您面对的是一个没有日志记录的VPN，一个能消除或至少不存储您的使用记录的VPN。除此之外，检查网站—— 您通常用来下载客户端和提交信息的地方—— 不存储 cookies，以及它不会以任何其他方式跟踪您的数据，也很重要。 https://iyouport.substack.com/p/90vpn

做出正确的决定

挑选VPN并不像挑选家具。错误的决定会让您付出代价。不过，考虑到以上五点，您应该能够做出更明智的决定。

[image]
[image]

如果您的手机被盗或被警察抢走...

[image] 关键词	个人 反侦察 反取证 威胁响应 恶意软件 移动设备 预防性
[image] 关联	自卫措施
[image] 创建时间	2021年8月5日
[image] Description	操作安全性

非常重要的事尽可能不要在手机上完成。但即便您只有手机没有电脑，也有一些方法可以缓解被警察和窃贼 抢走手机的后果。

- Table of Contents

  没有物理访问您的手机的人可以知道您的什么？
  为了防止这种情况的发生：
  有物理访问权的人可以知道什么？
  如果您的手机找回来了呢？

[image]

本文是给大众的，也就是最常见的使用手机的人们。对于从事极度敏感活动的人，比如吹哨人、人权律师、活动家等等，您需要更有针对性的措施；但基础框架是一样的。

[image]

激进社区用户请从这里进入：[image]匿名手机 ；周密的行动计划 ；分身 ；[image]计算机和移动设备取证 ；[image]计算机和移动设备取证 ；加密 ；[image]物理入侵检测 ；[image]突袭应对措施 ；[image]防篡改准备

您的手机就是您的全部生活。在这里，您可以进行交流，获取新闻，为您所爱的人拍摄照片和视频，放松身心，玩游戏，等等。它可以跟踪您的健康状况，为您指路，提醒您发生的事件，以及更多。

于是，手机很容易被恶意行为者用来对付您。

[image]

重要的是要知道您的手机包含什么，以及它如何导致您容易受到攻击。

您的威胁模型是独特的，也是个人化的。这意味着您将不得不自己来决定哪些解决方案最适合您。

最好的保护是避免给攻击者创造任何机会，使其能够物理访问您的手机或其元数据。最安全的解决方案是不要将手机带入任何高风险活动中，比如抗议活动，但这对每个人来说可能并不可行。

没有物理访问您的手机的人可以知道您的什么？

在没有攻击者对您的手机进行任何物理访问的情况下，您可能认为您的隐私是安全的。但是，您的手机不断地与手机信号塔进行通信，以便能够传输数据（用于浏览或应用程序），或接收和发送短信或电话。要做到这一点，网络需要知道哪个手机塔在给您服务。

换句话说，网络知道您在哪里。这使得能够访问您的服务提供商所持有的位置数据的所有人都能够知道您的位置和移动路径。

为了防止这种情况的发生：

- 飞行模式将禁用与蜂窝网络的通信—— 如果您的手机不与蜂窝网络通话，就无法通过这种方式追踪您的位置。确保WiFi和蓝

牙也被禁用，因为它们也可能泄露信息。然而，这也意味着您将无法使用数据或获取信息或电话。

- 避免使用短信或普通电话—— 这些都没有加密，连同您的位置，可以被您的服务提供商看到，他们可以使用黄貂鱼拦截您的数据。您需要使用安全的端对端加密信息传递。

有物理访问权的人可以知道什么？

通过物理访问您的手机，攻击者可以获得手机中存储的所有数据。这其中包含了您的通信、照片、浏览历史和应用程序。但它也包含了更多的内容，比如：

- 电话通话记录
- 短信，这包括短信/彩信和任何其他的消息应用程序，只要您安装了
- 日历和笔记
- 照片/视频/音频
- 密码，如果存储不安全，或者如果攻击者也能访问您的密码管理器（如果您使用了一个弱的主密码、指纹或Face ID，或者您的密码管理器在警察没收您的设备时被解锁，就有可能出现这种情况）
- 账户登录
- 云数据和备份《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》

- 已经删掉的数据。即使您从手机中删除了一些东西， 它仍然可以活在许多地方，在内存和日志中，它可以被恢复。《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》

- 应用切换屏幕截图。当您切换或关闭一个应用程序时，许多设备为您提供了一个正在运行的应用程序的概述，以及他们正在或曾经在做什么。为了实现这一点，他们所做的是创建应用程序内屏幕上发生的最后一件事的截图。该截图会被存储起来，攻击者可以检索到它。一些应用程序会混淆这一点，但大多数不会。这可能会暴露加密通信、密码或其他私人信息

- 位置。您的手机会不断地记录很多细节来显示您的行踪，比如您加入的WiFi接入点、您的手机服务的记录、您拍照时的坐标等等；许多应用程序使用您当前的位置来提供 “相关” 的搜索结果、天气更新，或其他任何东西

- 日志。您的手机和应用程序有各种各样的文件，记录着它所做的事，错误和崩溃。所有这些信息都被存储起来，可以揭示您如何使用手机，您与谁联系，以及您在哪里。这是一个庞大的列表，为攻击者提供了大量的关于您的私密信息 ……

[image]

激进社区用户请从这里进入：[image]计算机和移动设备取证

不用说，您需要保护您的数据和对手机的访问权限。最好的方法是启用全盘加密并使用强密码。并非所有的设备都一样，您需要验证您的设备是否提供全盘加密。

最新版本的Android和iOS默认提供全盘加密。为了确保它的启用，您将不得不添加一个强密码。不要使用只有数字的密码或任何弱密码，因为有许多工具可以轻松破解它们。如果您的手机有一个SD卡，这也可以包含信息，可能不会被您的设备加密。

法院可以批准在未经您的同意的情况下解锁受生物识别（如人脸或指纹识别）保护的手机，因此建议不要启用这两个选项。如果这不可

行，切断设备电源，在重新开启时大多数设备都会要求输入密码。

小心使用云备份。虽然恢复您的应用程序和备份消息和图像很有用，但是它们也可以为攻击者提供获取数据的便捷途径。或者，如果攻击者已经可以访问您的手机，他们可以使用您的备份来恢复旧信息，如照片和信息的备份。如果可以的话，在高风险场景下（如参加抗议活动/或可能遇到警察查手机的情况下）禁止访问云。

- 使用强密码对设备进行全盘加密
- 禁用人脸识别和指纹识别
- 禁用云备份
- 关机

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

如果您的手机找回来了呢？

假设您的手机被警察拿走了，然后他们又还给您了。您应该怎么做？

最简单的方法就是：弃用。如果您能负担得起，而且您的威胁模型包括这点：那就换一部新手机。

否则：

- 更改所有的密码
- 验证是否有人访问过您的账户。一些电子邮件提供商和社交媒体网站会显示访问您账户的IP列表）。

- 恢复出厂设置。确保您知道这样做对您的特定设备意味着什么。有些情况下会擦除加密的主密钥，有些则会保留一些数据。您需要擦除所有的数据。

- 用新的Apple ID/Google账户登录手机，以避免加载可能受到损害的云端备份。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

[image]
[image]

如何保护自己免受蔓延全世界的最强大的以色列间谍软件 **Pegasus** 的攻击

[image] 关键词	以色列 数字卫生 自卫 间谍软件
[image] 关联	[image]当您准备像编程随想那样工作…：须知 ；[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法
[image] 创建时间	2021年9月8日
[image] **Description**	操作安全性

安全性虚无主义是最可怕的事，其危险程度超过攻击本身。

- Table of Contents

1、网络注入
2、**Bridgehead**
3、照片
4、**iMessage** 中的无交互**0-day**问题
5、苹果音乐
6、工具和援助
Pegasus 提供 “对目标移动设备的无限制访问”
1、躲避社交工程的诱饵
下面是一些例子，说明这在实践中意味着什么：
2、挫败网络注入攻击
3、零点击漏洞
具体来说，用户可以这样做：
4、物理访问
以下是你可以如何减轻它们的影响的一些方法：

关于大赦国际发布的移动验证工具包

[image]

人们曾经认为只有极高级别的敏感人士才会遭遇到最昂贵和最可怕的间谍软件，而这一假设在今年夏天被一场惊人的数据泄露所推翻；调查显示，以色列最恐怖的监视技术公司 **NSO** 的 **Pegasus** 间谍工具通过利用苹果软件的弱点，包括 **iMessage** 的无交互零日漏洞，渗透到全世界的记者、律师、人权捍卫者、活动家、和企业高管的 **iPhone** 手机中。

这是今年6月最火爆的消息之一，虽然，它并不是新闻 —— 我们的原网站有 https://start.me/w/8LRjvQ 专栏。但很少有人会思考该如何应对这种可怕的攻击。这是本文希望尝试解释的问题。

虽然NSO一直在狡辩，声称该间谍软件“只用于打击罪犯”，但6月泄露的潜在目标清单显示，记者、活动家和政客都是被NSO的客户瞄准的对象。

大赦国际描述说，这些详细的攻击从2014年一直持续到2021年7月。一些攻击被认为是“零点击/无交互”，即 受害人不需要以任何特定的方式进行互动就能被成功攻击。

该间谍软件还使用了多个零日漏洞，包括运行 iOS 14.6 系统的 iPhone 12。

[image]

全世界的政府都在囤积零日漏洞，它可能是本世纪最强大的政治武器。这件事非常重要：

事实上，大赦国际报告中列出的攻击早在**2018**年**5**月就开始了 —— 也就是**IYP**开始报告这一系列灾难的最初时间。

[image] [image]

[image]

延伸：https://iyouport.substack.com/p/130lgbt?utm_source=publication-search

延伸：https://iyouport.substack.com/p/lr-nso-pegasus-45-?utm_source=publication-search

正如约翰霍普金斯大学的密码学家马修格林所担心的，这一披露有可能让黑客专家们陷入“安全性虚无主义”的境地。

安全性虚无主义认为，数字攻击已经变得如此复杂，以至于没有什么可以防止它们发生的，也无法削弱其影响。这种结论将是一个错误。

我们在解释IYP为什么采取开源情报的时候提到过中国社会的安全性虚无主义，并且这一现象至今都明显存在着，BACK https://iyouport.substack.com/p/lr-iyp?utm_source=publication-search。

[image]

任何时候，知道永远比不知道要强，

我们需要冷静下来仔细思考可能的对策。

虽然说实话，除非跨国联合的革命推翻这一弥漫全球的政治武器，

否则，单纯的技术弥补并无法成为长期出路。

首先，虚无主义正中了恶意黑客的下怀，他们最希望看到的就是目标不再试图保护自己。并且，这在事实上也是错误的。您依旧有可能抵御NSO的间谍软件—— 例如，通过遵循操作安全规则，比如最简单的不点击未知链接，实行设备分区（如为不同的应用程序使用不同的设备），以及在移动设备上安装加密VPN，等等。这些技术对任何数量的数字攻击都是有效的。

[image]

激进社区用户请从这里进入：[image]数字技术限制和最佳实践

正如安全领域的一句经典格言所说，并没有百分百完美的安全性，但这并不是消极怠工的借口。那么，以下是一些您可以采取的实际步骤，以减少您的“攻击面”，保护自己免受像**NSO**这样的间谍软件的侵害。

此外，最近，公民实验室也做了一份调查报告，有技术分析，您可以参考 https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/

[image] 德国警方秘密购买了 NSO Pegasus 间谍软件 消息来源证实媒体报道称，联邦刑事警察不顾律师的反对，购买并使用了备受争议的以色列监控间谍软件 —— 德国联邦刑事警察局 (BKA) 于 2019 年从以色列公司 NSO 购买了臭名昭著的 Pegasus 间谍软件。议会消息人士称，联邦政府在闭门会议上将此次购买通知了联邦议院内政委员会。这证实了早先在德国《时代周报》上发表的报道。据 Die Zeit 称，该软件是在“极度保密”的情况下采购的，尽管律师们犹豫不决，因为该监控工具的功能远远超出了德国隐私法所允许的范围。
[image] [image] 巴林政府使用 NSO 恶意软件来攻击活动家和持不同政见者

我们首先来看看它的攻击方式。

1、网络注入

第一类攻击是网络注入，即 用户被神秘地从一个合法网站重定向到另一个。Safari浏览器的浏览历史日志显示了被访问了的可疑URL，这是打开网页后几乎不到一秒钟内就发生的被重定向的证据。

[image]

Favicon 数据库也显示了类似重定向的证据，尽管不一定是通过主动浏览。在一个案例中，尽管没有打开单独的浏览器，但在预览一个记者的 Twitter 时间线中分享的链接时，使用的Safari浏览器服务促使网页加载并重定向到可疑的URL。

2、Bridgehead

进程执行的记录显示，名为 “bh” 的进程也与 Pegasus 安装域有关，通常在成功的网络注入尝试后出现。

据认为，“bh” 与 iOS JavaScriptCore 二进制中的一个2016年的漏洞有关，该漏洞使代码得以执行，并在重新启动后在设备上保持持久性。bh 被认为代表 “BridgeHead”，是该组件的内部名称。

在 “bh” 之后，该恶意软件还使用了其他进程，包括 “roleaboutd” 和 “msgacntd”，它们被认为是在成功利用和特权升级后使用的后期进程。还发现了其他类似的进程，包括 “pcsd” 和 “fmld”，它们可能有相同的目的。

3、照片

有证据显示，在使用 “bh” 进程之前，苹果公司的一个名为 “mobileslideshow” 的照片应用程序进程可能已被用于攻击中。

人们怀疑 Photos 应用程序或 Photostream 服务被用作部署 Pegasus 间谍软件的漏洞利用链的一部分。

在每一个使用 Photos 的案例中，似乎 Photostream 使用的是同一个iCloud账户地址。一些无交互攻击显然需要特定的iCloud账户才能发挥作用。

4、iMessage 中的无交互0-day问题

从2019年开始，iMessage 和 FaceTime 中的许多漏洞被发现和修补，但是，似乎有些问题仍然可以被滥用。

在一次攻击中，人们发现可疑的 iMessage 账户查询后执行了 Pegasus 间谍软件进程。多个匈牙利记者显然是同一操作者的目标，每次攻击都使用了类似的地址和进程。

通过 iMessage 的攻击显然在2021年又回来了，这次涉及到一个可疑的 iMessage 账户的查询，然后是一个 coretelephony 进程执行的HTTP请求。这似乎是为一个名为 “gatekeeperd” 的进程请求一个有效载荷。

2021年5月的一次攻击显示，对一个神秘的iCloud账户进行了类似的查询，推送通知显然被用作在执行前将有效载荷应用到目标iPhone上的一种方式。

5、苹果音乐

还有证据表明，Pegasus 间谍软件可能在2020年7月通过苹果音乐应用程序交付。在那次感染中，苹果音乐的网络流量被记录下来，音乐应用程序的HTTP请求再次指向用于分发 Pegasus 的域。

大赦国际无法确定苹果音乐本身是否被用于最初的感染，或者它是否被用于沙盒逃逸或特权升级。

6、工具和援助

调查结束后，大赦国际通过 GitHub 发布了 Pegasus 指标，以协助其他安全研究人员发现其他 Pegasus 感染。这些指标包括 Pegasus 基础设施中的域名、从 iMessage 账户查询中恢复的电子邮件地址，以及与该软件相关的进程名称。

名为 “移动验证工具包” 的工具也正在发布。作为一个模块化的工具，它旨在简化获取和分析来自安卓设备的数据的过程，以及分析来自iOS备份和系统转储的记录，以找到任何进一步的潜在痕迹。

[image]

Pegasus 提供“对目标移动设备的无限制访问”

最近披露的信息涉及NSO的一个特定的间谍软件产品，即 Pegasus。在这之前，公民实验室、国际特赦组织、Article 19、R3D 和 SocialTIC 等机构都对该公司的监控工具进行了广泛研究。以下是一些具体了解。

该间谍软件的功能在似乎是**NSO**集团**2014**年或更早的宣传手册中就有所概述，并在 **WikiLeaks** 公布与另一家间谍软件公司**——** 意大利 **Hacking Team——** 有关的电子邮件库时提供。该文件积极地推销 Pegasus，说它提供“对目标移动设备的无限访问”，并允许客户“远程和隐蔽地收集有关你的目标的关系、位置、电话、计划和活动的一切信息 —— 无论何时何地”。

该手册还指出，Pegasus 可以：

- 实时监控语音和VoIP电话；
- 从手机中吸取联系人、密码、文件、和加密的内容；
- 作为一个“环境窃听器”操作，通过麦克风进行监听；
- 通过 WhatsApp、Facebook、Skype、Blackberry Messenger 和 Viber 等应用程序监控通信；
- 通过GPS追踪手机的位置……

然而，尽管大肆宣传，Pegasus 依旧只是一种被称为远程访问木马或RAT的旧式恶意软件的美化版本：一种允许未授权方完全访问目标设

备的程序。换句话说，虽然 Pegasus 可能是强大的，但理论上安全界应该很清楚如何防御这种类型的威胁。

让我们来看看 Pegasus 可能感染手机的不同方式 —— 用该手册上的说法，它的各种“代理安装载体” —— 以及如何抵御每一种。

1、躲避社交工程的诱饵

社交工程手段始终都是安全威胁的要点，是攻击者第一步需要使用的突破口。社交工程学也是审讯心理学的主体，以帮助被捕和被喝茶的人防止被警察套话。在安全角度上它很重要，您可以在本站的 心理安全-PsychologicalSecurity 专题中看到相应的防御策略推荐。

在关于 Pegasus 攻击的报告中，有许多记者和人权维护者收到了短信和 WhatsApp 诱饵信息，引诱他们点击恶意链接。这些链接会下载间谍软件，通过浏览器和操作系统的安全漏洞进入设备。还记得华盛顿邮报专栏作家 Jamal Khashoggi 是如何被分尸的吗 —— 是的，只因为他的亲密队友在网店订购了一罐蛋白粉。在这里看到这个故事 https://iyouport.substack.com/p/4bc。

在泄露的间谍软件手册中，这种攻击媒介被称为“增强型社交工程师信息”（**ESEM**）。它指出，“目标将点击链接的机会完全取决于内容的可信度水平。**Pegasus** 解决方案提供了广泛的工具来编写一个*量身定制*的看起来完全无害的信息，以引诱目标点击”。

正如保护记者委员会所详述的，与 Pegasus 有关的ESEM诱饵信息分为不同的类别。有些声称是来自银行、大使馆、新闻机构、或包裹递送服务等既定组织。其他的则与个人事务有关，如工作或所谓的伴侣出轨证据，或声称目标人物正面临一些直接的安全风险。

未来的ESEM攻击可能会使用不同类型的诱饵信息，这就是为什么你必须谨慎对待任何试图说服你执行数字动作的信息和信件。

下面是一些例子，说明这在实践中意味着什么：

A、如果你收到带有链接的信息，特别是如果它包含一种紧迫感（说明一个包裹即将到达、或你的信用卡将被扣款），你必须避免自己立即点击它的冲动。

B、如果你信任所链接的网站，请手动输入链接的网址，而不是直接点击。

C、如果要去一个你经常访问的网站，将该网站应该被保存在一个本地的书签文件夹中，并且，你应该只从你自己的文件夹中的链接访问该网站。

D、如果你决定要点击一个链接，而不是在浏览器中键入它或通过书签访问该网站，至少要仔细检查该链接，以确认它是指向一个你熟悉的网站。请记住，你仍有可能上当受骗：一些钓鱼网站的链接使用非英语字符集中看起来相似的字母，这就是所谓的同形异义字。例如，西里尔字母 “O” 可能被用来模仿在英语中通常看到的拉丁字母 “O”。

E、如果该链接看起来是一个缩短的URL，请使用**URL**扩展器服务，如 ExpandURL，在点击前显示其指向的实际长链接是什么。

F、在你点击一个显然是由你认识的人发送给你的链接之前，请确认这个人确实是你认识的那个人、此人确实给您发送了这个链接；因为你的朋友的账户可能被黑了，或者他们的电话号码被伪造了。要使用与你收到该信息时不同的通信渠道向你的朋友确认这件事。例如，如果链接是通过短信或电子邮件发送的，那就给发件人打个电话。这就是所谓的“频外认证或鉴定”。

G、实行设备隔离，使用一个没有任何敏感信息的辅助设备来打开不受信任的链接。请记住，如果辅助设备被感染，它仍然可能被用来通过麦克风或摄像头监控你！所以在不使用时将其放在法拉第袋中 ——或者至少远离你进行敏感对话的地方（放在法拉第袋中肯定是个好主意）。

H、使用非默认的浏览器。根据泄露的 Pegasus 手册中题为 “安装失败” 的部分，如果目标人运行的是不支持该间谍软件的浏览器，特别是 “设备的默认浏览器” 以外的浏览器，安装可能失败。但是，请注意！这份文件已经是几年前的了，而且今天的 Pegasus 可能已经可以支持所有种类的浏览器。

I、如果对某个链接有任何怀疑，最安全的措施是避免打开该链接。

2、挫败网络注入攻击

在多个案例中，Pegasus 感染设备的另一种方式是通过拦截手机流量，即所谓的中间人攻击或MITM，其中Pegasus拦截未加密的网络流量，如HTTP网络请求，并将其重定向到恶意的有效载荷。

要做到这一点，间谍软件需要欺骗手机连接到一个假装是附近手机塔的流氓便携设备 —— 就如[image]黄貂鱼；或者，直接获得对目标手机运营商的访问权（ [image]服务提供商协助调查 ）。即使手机处于仅有移动数据的模式，并且没有连接到**Wi-Fi**，这种攻击也能发挥作用。

当非政府组织 FreedomNow 和摩洛哥调查性新闻协会的联合创始人 Maati Monjib 打开 iPhone Safari 浏览器并输入 yahoo.fr 时，Safari 首先尝试转到 http://yahoo.fr。通常情况下，这将重定向到 https://fr.yahoo.com，一个加密的连接。但是，由于 Monjib 的连接被拦截了，它反而重定向到了一个恶意的第三方网站，并最终入侵了他的手机。

如果您在浏览器地址栏中只输入网站域名（如 **yahoo.fr**）而没有指定协议（如 **https://**），这就为**MITM**攻击提供了可能，因为您的浏览器默认会尝试以未加密的**HTTP**连接到该网站！通常情况下，您到达真正的网站时，它立即将您重定向到一个安全的HTTPS连接；但是，如果有人跟踪并黑进您的设备，第一个HTTP连接就足以成为劫持您的连接的入口。

一些网站使用一种被称为HTTP严格传输安全性的复杂安全功能来防止这种情况，这可以防止您的浏览器向他们发出未加密的请求，但是，您不能总是指望这一点，即使对于一些能够正确实施它的网站而言也是如此。

这里有一些您可以做的事，以防止这些类型的攻击：

- A、在进入网站时，一定要键入 **https://**

- B、将你喜欢的网站的安全（HTTPS）网址加入本地书签，并使用这些网址来访问网站，而不是直接输入域名。

- C、另外，在您的桌面和移动设备上都使用**加密的VPN**。VPN将所有连接安全地传输到VPN服务器，然后代表你访问网站并将其转发给你。这意味着监视你的网络的攻击者很可能无法成功地进行MITM攻击，因为你的连接是加密到VPN 的 —— 即使你在浏览器中直接输入了域名而没有带 “https://” 部分。

但如果你使用VPN，请始终记住你的VPN供应商有能力监视你的互联网流量，所以，挑选一个值得信赖的供应商非常重要—— 在这里看到 [image]某个VPN可能不可靠的5个标志：如果您不理解技术的话 。

此外，Wirecutter 根据VPN供应商的第三方安全审计历史、他们的隐私和使用条款政策、所使用的VPN技术的安全性以及其他因素，发布了定期更新的、全面的VPN供应商比较。您可以参考。

3、零点击漏洞

与需要目标执行某些行动（如点击链接或打开附件）的感染企图不同，零点击漏洞之所以被称为零点击，是因为它们不需要目标的任何互动。所需要的只是目标人安装了一个特定的脆弱的应用程序或操作系统。如前文所示，大赦国际对最近披露的 Pegasus 证据的取证报告指出，一些感染是通过利用苹果音乐和 iMessage 应用程序的零点击

攻击传播的。

这不是NSO集团的工具第一次与零点击攻击有关。2017年针对巴拿马前总统里卡多·马蒂内利的投诉就指出，记者、政治人物、工会活动家和公民协会领导人都已经成为 Pegasus 间谍软件的目标，而在2019年，WhatsApp 和 Facebook 提出投诉，称NSO集团开发的恶意软件能够利用 WhatsApp 的零点击漏洞。

由于零点击漏洞 / 即 无交互漏洞，顾名思义就是不需要任何用户互动，它们是最难防御的。但是，用户可以通过减少所谓的“攻击面”和实行设备隔离，来减少被这些漏洞击中的机会。

减少您的攻击面仅仅意味着最大限度地减少您的设备可能被感染的方式。设备隔离意味着将您的数据和应用程序分散到多个设备上——中国用户应该很容易理解这点，我们曾经多次听闻中国用户将微信、微博、支付宝等中国流行应用隔离到一台单独的设备上，这是非常好的。

具体来说，用户可以这样做：

- A、减少你手机上的应用程序的数量。

你家里未上锁的门越少，窃贼进入的机会就越少；同样，较少的应用程序意味着你手机上可供对手利用的虚拟门越少。你的设备应该有你执行日常功能所需的最基本的应用程序。

如果有一些应用程序你不能删除，比如 iMessage；在这些情况下，你通常可以禁用它们，尽管这样做也会使文字信息在你的 iPhone 上不再起作用。

- B、定期检查你安装的应用程序（和它们的权限），并删除任何你不再需要的应用程序。

删除一个很少使用的应用程序，并在你真正需要它时再次下载它，比

让它留在你的手机上更安全。不要忘了 [image] 少即是多：变得难以被追踪的简单方法 S03E05 。

- C、及时更新，越快越好。

及时更新手机操作系统和个别应用程序，因为更新可以弥补漏洞，有时甚至是无意的漏洞。

- D、将你剩余的应用程序分门别类。

如果一部手机只安装了 WhatsApp 并被入侵，黑客会得到 WhatsApp 的数据，但不会得到其他敏感信息，如电子邮件、日历、照片或 Signal 加密信息。

- E、物理隔离。

普通包裹并没有用，手机仍然可以被用作窃听和跟踪设备，所以，要保持设备的物理隔离—— 也就是说，把它们放在另一个单独的房间里，最好是放在法拉第袋里。如果您曾经参加过具有保密级别的会议或进入安全设施内，您就会知道这点，手机是不能带入房间的。

[image]

激进社区用户请从这里进入：[image]户外无设备对话

4、物理访问

攻击者感染手机的最后一种方式是通过与目标手机进行物理交互 ——即 [image]恶意女仆和查抄 。根据该手册，“当物理访问设备是一种选择时，**Pegasus** 特工可以在五分钟内手动注入和安装”—— 尽管不清楚手机是否需要解锁，或者攻击者是否能够感染甚至是受密码保护的手机。

[image]

激进社区用户请从这里进入：[image]防篡改准备 ；[image]藏匿点或安全屋 ；[image]突袭应对措施 ；[image]物理入侵检测

目前似乎还没有已知的物理发起 Pegasus 攻击的案例，尽管这样的漏洞可能很难被发现，很难与在线攻击区分开。

以下是你可以如何减轻它们的影响的一些方法：

- A、始终保持让你的设备在你的视线之内。

任何时候，只要你的设备离开你的视线，就有可能发生物理上的破坏。不论是去洗澡还是如厕，只要房间里还有另一个人，或者，有任何人可能进入这个房间，就最好随身携带你的所有电子设备。

显然，海关人员在机场可以拿走你的手机，这和你去洗手间时把笔记本电脑留在卧室里是有区别的，但都涉及一些同样的风险，你将不得不校准自己的风险承受能力。

- B、当设备不得不无人看管时，把它放在法拉第袋里，特别是在酒店房间等风险较大的地方。

这并不能防止设备被操纵，但至少可以随时提醒你，设备已经从袋子里被拿出来了，可能被人动过了，这时就不应该再使用该设备。

- C、敌我有别。

在进入潜在的敌对环境，如政府大楼，包括大使馆和领事馆，或通过边境检查站时，请使用一次性电话和其他隔层设备。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

返回：[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

一般来说：

A、如果你怀疑自己的手机感染了 Pegasus，请使用大赦国际的移动验证工具包。

B、定期备份重要文件。

C、定期重置你的手机也没有坏处。

尽管 Pegasus 是一个极度危险和复杂的间谍软件，但请相信你可以采取一些具体的步骤来尽量减少自己的设备被感染的机会。没有万无一失的方法可以完全消除风险，但你肯定可以做一些事来降低这种风险，安全虚无主义是要不得的。

[image]

关于大赦国际发布的移动验证工具包

大赦国际发布了一个工具，可以帮助您检测自己的手机是否受到影响。

该工具包旁边是一组很棒的说明，应该可以帮助您完成一些技术检查过程。使用该工具涉及将手机备份到单独的计算机，并对该备份运行检查。下面做一些介绍。

首先要注意的是，该工具是基于命令行或终端的，所以它将需要一定的技术能力或一点耐心来运行。但真的不难！请放心，按照说明做就行了。下文将试图涵盖很多你需要知道的东西。

第二个说明是，大赦国际正在运行的分析似乎对iOS设备效果最好。大赦国际在其文件中说，其工具可以在安卓手机备份上运行的分析是有限的，但该工具仍然可以检查潜在的恶意短信和APK。同样，建议遵循其说明。

要检查您的 iPhone，最简单的方法是在Mac或PC上使用 iTunes 或 Finder 做一个加密的备份。然后您需要找到该备份的位置，苹果公司提供了相关的说明。Linux 用户可以按照大赦国际的说明，使用 libimobiledevice 命令行工具来创建备份。

获得手机备份后，需要下载和安装大赦国际的mvt程序，大赦国际也提供了相关说明。

如果您使用Mac来运行检查，首先需要安装 Xcode（可以从App Store下载）和 Python3，然后才能安装和运行mvt。 获得 Python3 的最简单方法是使用一个叫做 Homebrew 的程序，它可以从终端安装和运行。安装完这些后，您就可以运行大赦国际的iOS指示了。

如果您在试图解密您的备份时遇到问题，没关系。当我试图把它指向我的备份时，该工具也报错了，我的备份在默认文件夹中。为了解决这个问题，我把备份文件夹从默认位置复制到桌面上的一个文件夹里，并把mvt指向它。命令最后看起来像这样：

```
mvt-ios decrypt-backup -p PASSWORD -d decrypt ~/Desktop/bkp/orig
```

【注：请注意，这仅用于说明目的。请使用大赦国际给出的命令，因为程序可能已更新】

当运行实际扫描时，您要指向一个 “Compromise” 文件，大赦国际以一个名为 pegasus.stix2 的文件形式提供。那些刚开始使用终端的人可能会被如何实际指向一个文件所困扰，但只要您知道文件的位置，这是相对简单的。对于初学者来说，建议将 stix2 文件下载到您的Mac的下载文件夹。然后，当您到了实际运行检查-回溯命令的步骤时，添加：

```
-i ~/Downloads/pegasus.stix2
```

进入选项部分。作为参考，这里的命令最后看起来像下面这样。(同样，这只是为了说明问题。如果您只是复制这些命令并运行它们将导致错误）：

```
mvt-ios check-backup -o logs—iocs ~/
Downloads/pegasus.stix2 ~/Desktop/bkp/decrypt
```

(作为参考，~/ 或多或少地充当了您的用户文件夹的快捷方式，所以您不必在 /Users/mitchell 这样的地方添加什么)

再一次，建议您按照大赦国际的指示，使用其命令，因为该工具总是有可能被更新。安全研究员 @RayRedacted 在Twitter上也发布了一个很好的 thread，讲述了您在运行该工具时可能遇到的一些问题以及如何处理它们。

最后，大赦国际只提供了在 MacOS 和 Linux 系统上安装该检测工具包的说明。对于那些希望在Windows上运行它的人来说，The Verge 已经证实该工具可以通过安装和使用 Windows Subsystem for Linux（WSL）并遵循大赦国际的 Linux 说明来使用。使用WSL将需要下载和安装一个Linux发行版，如 Ubuntu，这将需要一些时间。不过，它可以在您等待手机备份的时候完成。

运行mvt后，您会看到一个警告列表，其中列出了可疑的文件或行为。值得注意的是，警告并不一定意味着您已经被感染了。对我来说，一些完全正常的重定向出现在它检查我的 Safari 历史的部分（sheet.google.com 重定向到了 docs.google.com，reut.rs 重定向到 reuters.com，等等）。同样，也会得到一些报错，但只是因为该程序正在检查我的手机上没有安装的应用程序。

围绕 Pegasus 的故事可能会让许多人对手机这种担心比平时多了几分怀疑，不管您是否有可能成为一个民族国家的目标。

正如您已经看到的，政府有可能并不需要入侵您的手机的麦克风和摄像头，就可以获取您的私人信息 —— 即使您的手机没有感染 **Pegasus**，无孔不入的数据中介行业也极有可能已经在出售您的位置历史记录了。这里有一个具体说明，您真的有必要仔细阅读 **[image]** 单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

[image]
[image]

如何检查MacOS上的恶意软件和键盘监听程序

[image] 关键词	恶意软件 电脑 自检
[image] 关联	[image]免费的macOS清洁软件；[image]设备好像被黑了怎么办？ - 数字急救包
[image] 创建时间	2021年12月28日
[image] **Description**	操作安全性

非常简单的工具，任何人都可以使用。

- Table of Contents

适用于**MacOS**的恶意软件
ReiKey 和 **KnockKnock** 可以检测新型恶意软件
您需要什么
第一步：从 **Objective-see.com** 下载工具
第二步：安装 **ReiKey**
第三步：扫描键盘监听器
第四步：安装 **KnockKnock**
第五步：扫描您的**MacOS**系统
第六步：检查可疑的东西
键盘监听程序和持久性恶意软件可能是一个严重的问题

[image]

虽然您可能怀疑您的 MacOS 已感染了恶意软件，但可能很难确定。本文来说说这件事怎么做。

发现恶意程序的一种方法是查找可疑行为，例如 恶意程序在键盘输入时监听。

借助免费的 MacOS 工具 ReiKey 和 KnockKnock，您可以检测可疑程序，以发现潜伏在系统中的键盘监听和其他持久性恶意软件。

键盘监听或恶意软件可以通过多种方式最终出现在MacOS系统上。它可能来自受感染的文件、USB Rubber Ducky 黑客等等。

重视个人隐私的任何人都应该关注确保通信不会被恶意拦截。那么 MacOS 究竟有多少恶意软件？

适用于MacOS的恶意软件

创建 MacOS 安全工具的前国家安全局黑客 Patrick Wardle 研究了为 Apple 设备编写的恶意软件。Patrick 在其网站上托管了 MacOS 恶意软件的实时样本供研究人员研究，在野外发现的各种恶意软件令人震惊。

对 keyloggers 的简单搜索就可以找到五种用于 MacOS 设备的键盘监听恶意软件。

[image]

这就提出了一个挑战：既然键盘记录程序至少具有五种不同的风格，我们如何防御所有这些不同类型的恶意软件？

Wardle 的答案是搜索诸如键盘记录程序之类的恶意程序的行为，而不仅仅是搜索程序本身。

例如，一个键盘监听器从您的键盘上窃听了事件流，从而使攻击者可以截获受害者键入的每个键。这将使他们能够获知帐户密码、拦截通信等。

但是，要真正生效，这些程序必须在您登录计算机后立即运行。这意味着恶意程序通常会永久安装，不需要受害者每次都误点击恶意文件。

ReiKey 和 KnockKnock 可以检测新型恶意软件

首先，ReiKey 允许您搜索键盘监听器的最基本特征之一：深入键盘流窃听的程序。寻找键盘流访问功能将使您能够警觉到系统上安装的所有键盘监听器，而不仅是防病毒程序可识别的键盘监听器。

此外由于键盘监听器也将永久安装，因此可以使用另一个名为 KnockKnock 的免费工具来发现它。

运行 KnockKock 时，它将持久安装的程序分为易于理解的类别。包括恶意软件通常会用来持续运行的程序类型：浏览器扩展、启动项、内核扩展和插件。

[image]

扫描系统后，KnockKnock 将识别每个永久安装的项目并检查是否已在 VirusTotal 中进行了标记。

[image]

如果恶意程序潜伏在您的系统中，则可以通过单击 “Info” 图标来进一步研究细节。

如果您发现由 VirusTotal 标记的文件并且看起来可疑，这充分表明您的系统已受到恶意软件、广告软件或其他有害程序的破坏。

下面测试下这些程序，看看可以在 Mac 上找到什么。

您需要什么

要使用 KnockKnock 和 ReiKey，您只需要一个最新版 MacOS 系统来安装它。您还需要互联网连接和浏览器才能下载安装程序。

第一步：从 **Objective-see.com** 下载工具

首先，在 Objective-see.com 上导航至 ReiKey 的产品页面，然后在页面左上方的 ReiKey 图标下找到下载链接。

[image]

下载安装程序并解压缩。双击 “ReiKey Installer.app” 文件以启动安装。

第二步：安装 **ReiKey**

安装程序打开后，只需点击 “安装” 按钮即可在 MacOS 系统上安装 ReiKey。

[image]

安装完成后，点击 “下一步” 以关闭安装程序。现在，您的任务栏中应该有一个 ReiKey 图标。

[image]

点击任务栏中的 ReiKey 图标，然后点击 “首选项”。您可以在其中访问配置选项，允许您设置是否在登录时运行该程序，在状态栏中使用图标运行，以及在扫描时是否忽略 Apple 的程序。

[image]

当我运行 Python 键盘记录程序时，在设备上收到以下警报。

[image]

第三步：扫描键盘监听器

现在已经安装并配置了 ReiKey，可以运行扫描了。

再次点击状态栏中的 ReiKey 图标，这一次点击 “扫描” 选项。将会弹出一个窗口，显示扫描结果，显示是否有程序正窃听你的键盘。

[image]

在这里可以看到进程。如果您在此处看到某些内容，则意味着某个程序正在监听您的每次按键。

第四步：安装 **KnockKnock**

接下来将安装 KnockKnock 来查找持久性恶意软件。为此，请导航至 “ KnockKnock” 页面。在左上角找到该应用的下载图标。

[image]

下载 KnockKnock 后，您可以直接运行它而无需安装。

第五步：扫描您的**MacOS**系统

运行下载的 “KnockKnock.app” 文件，然后将打开以下窗口。

首先，单击箭头图标以启动扫描。如果您正在运行最新版本的 MacOS Catalina，则扫描过程将需要您授予它访问各种文件夹和程序的权限。

[image]

扫描系统中的文件后，将显示一个持久安装的程序列表。

可能会永久安装很多不是恶意的东西，因此请仔细检查每个结果以查看是否可以识别该程序。例如，如果您有未使用或无法识别的浏览器扩展，那么最好删除它们，不管它们是什么。

[image]

还可以识别具有可疑状态的程序。在这里，看到一个永久安装的脚本是未签名的，如解锁图标所示。

[image]

如果想仔细看一下，可以单击 “Info” 图标以显示更多详细信息。

第六步：检查可疑的东西

如果想仔细查看文件，可以通过点击 VirusTotal 分数来完成。分数将显示检出率和报告链接。如果要再次提交文件，请点击 “重新扫描” 。

[image]

重新发送将使您可以访问详细的报告。在这里，看到了发现的先前标记为未签名的 “Tor” 程序的检测报告。

[image]

看起来该文件不是恶意文件。但是如果确实是恶意文件，那说明您的工作很有效。

键盘监听程序和持久性恶意软件可能是一个严重的问题

普通 MacOS 用户可能难以识别自己计算机上的恶意软件。借助 ReiKey 和 KnockKnock，可以在安装后立即检测行为不佳的软件。

如果您担心被合作伙伴安装键盘监听程序、雇主对您的计算机进行监视、或者不必要的广告软件在周围闲逛并消耗内存，那么使用这些工具可以使 MacOS 系统免受间谍软件和持久性恶意软件的侵害。

[image]
[image]

如何跨社交媒体平台追踪目标人：对抗性思考方式

[image] 关键词	免追踪 开源情报 数字足迹 社交媒体 自检 追踪 防御
[image] 关联	🔍开源情报
[image] 创建时间	2021年12月28日
[image] Description	操作安全性

社交媒体情报和开源情报不完全相同，它们是包含关系，前者是后者的一个分支 —— 前者也是后者的基础。社交媒体情报是一切情报挖掘和现实追踪的关键；本文介绍的情报追踪工具是为提醒安全意识。

- Table of Contents

  介绍
  研究
  相同的帐户
  照片
  你说的每个字
  时间戳
  其他
  SocialPath
  局限性
  结论

这里介绍的是一个工具，叫 SocialPath，它可以根据名字搜集社交媒体情报。跨平台搜寻，检查 Twitter、Instagram、Facebook、Reddit

和 Stackoverflow。

收集到的数据按照词频、主题标签、时间轴、提及、相似的帐户进行排序，并在 D3js 的帮助下以图表形式显示。

这种技术使您可以跟踪不使用唯一昵称的暗网用户。

介绍

社交媒体情报（SOCMINT）是开源情报（OSINT）的核心，也是人工情报（HUMINT）的要素。

[image]

激进社区用户请从这里进入：🔍开源情报

如今，人们使用不同的平台来共享有关自己的信息，却没有意识到这些信息会如何暴露出自己的习惯、兴趣、位置和明显的见解 —— 这非常危险。

无数种机构包括政府间谍一直在广泛地使用社交媒体监视以观看特定的关键字、主题标签、使用信息建立支持情报的联系，并跟踪他们想要的任何人。

虽然这里面的动机并非都是邪恶的。

社交媒体情报 SOCMINT 在很多正义的事业上都非常有用，例如，twitter 僵尸网络跟踪、照片地理位置定位以识别虚假信息、或者查找并警告威胁因素的存在，等等。

早在五年前IYP创立之初我们就开始警告：切勿在各种不同的网络平台上使用相同的用户名/ID/照片和简介，因为这样做非常危险 ——

相当于给了监视跟踪一个极为便利的机会。

但直到如今，依旧有很多人在这样做。

如果您很受欢迎、是网络名人，并且希望仅通过自己的名字被他人认识，这可以说是很平常的事，但是，建议不要将暗网或黑客论坛中的身份与任何社交媒体服务混在一起，否则...... 那简直太糟糕了。

缺乏基本的操作安全性（**OPSEC**）是一切的灾难之源。

遗憾的是，直到目前为止低端的操作错误依旧非常普遍。

研究

刑事投诉、起诉书、司法部公告和其他相关的文件，有可能比安全技术更值得阅读，因为其中会透露很多关于政府间谍如何抓人和如何拿到证据的见解 —— 这些见解您可以在下面回顾我们曾经推荐过的内容：

[image]

延伸：https://start.me/w/65mjN4

阅读起诉书和司法文件不仅能够帮助您深入了解那些案例，并且，更为重要的是，您能从中得出很多经验和教训 —— 那些反侦察匿名工作失败的血淋淋的教训。

我刮了一个暗网论坛，以获取成员名录，然后在不同的社交媒体平台（如Facebook，Instagram，Twitter，Stackoverflow和Reddit）中寻找。值得一提的是，结果取决于您要监视的论坛是什么。

比如，您在马其顿暗网论坛中跟踪用户，那么调查本地的社交媒体服

务（仅在特定国家/地区流行的那些）就会非常有意义 —— 对中国来说尤其如此，因为中国墙内克隆了一个小世界。

另一方面，当您针对白俄罗斯论坛时，就没有必要考虑葡萄牙语服务。一些Darknet网站允许检查所有用户的声誉和帖子数量，而无需注册。这样就可以轻松排除掉某些帐户。

如果用户在服务之间重复其昵称，那就没有任何匿名性。

为了确认两个帐户（暗网和明网）都属于同一个人，请进一步分析照片、文字、时间戳或兴趣 —— 再次提醒，⚠语言指纹是非常危险的东西，即便您在其他方面保护得非常严谨，语言习惯也有可能暴露您！语言学取证已经是一个非常成熟的学科和一套迅速完善的技术。

您可以在下面这篇文章中看到所有您需要注意的危险漏洞，包括语言指纹，以及相关资料和视频：

[image]

返回：[image]袜子木偶 - 分身创建的小技巧

[image]

相同的帐户

为了证明上述，来看看美国起诉阿卜杜拉·阿尔玛什瓦利（Abdullah Almashwali）的案子：

[image]

查找与PGP密钥关联的电子邮件地址可以发现社交媒体资料。

之后，政府间谍获得了每个帐户的搜索授权书，其中包含详细信息和聊天记录。

这里的主要操作错误是：在电子邮件地址和社交媒体中使用了相同的昵称。此电子邮件可能还用于注册其他帐户（甚至所有账户）。

所有社交媒体网站都要随时配合政府间谍的需求 —— 请注意是所有！不分国家；仅仅是有些国家规定需要搜查令，而另一些国家可以随便拿。如果您知道搜查令有多么容易获得，就不会放松警惕了。

除了上面已经列举的教训之外，您还可以在下面找到更多案例；比如来自刑事诉讼，美国诉 Marcos Paulo De Olivieria-Annibale 案：

[image]

[image]

返回：[image]这些使用暗网的人是如何被抓到的？: 总结教训

照片

如上，您已经知道在不同平台使用相同的用户名有多糟糕；但是，您还需要知道，使用或发布相同的照片，比用户名更糟糕！

美国诉 HENRY KOFFIE a/k/a NarcoBoss 案表明，连接两个账户的指标之一是相同的资料图照片：

[image]

有时候一张照片顶得上千言万语。

例如 美国诉怀亚特·帕塞克（Wyatt Pasek）案表明，在确定犯罪嫌疑人的社交媒体账户后，一切都就非常清楚了。

任何时候，别得瑟！虚荣心会害死你 —— 请记住，名誉、金钱、他人的尊重、所谓的知名度和影响力……这一切都不是你的，命才是你的。

如果你要保命，就最好能放弃上述所有。

他们能用这种方法抓住毒贩，就能抓住他们想要的所有人。任何有点脑子和想法的人在当权者眼里都是敌人。

[image]

你说的每个字

也就是我们在前面强调过的 BACK [image]语言指纹 。

这类调查最有趣的方面就是按帐户对目标人使用过的字词进行对比分析。

因为每个人的脑回路都是有固定模式的，你平日可能没有注意到这点。于是，如果两个账户的操作者为同一个人，那么几乎肯定会漏出马脚。

语言学取证是非常专业的，并且只能由专业人员来得出结论，例如确认某人的原籍国、性情偏好、关联并揭示多重虚假身份等等。

某些字词、句子或成语，在不同国家/地区具有独特的含义，不同领域（工作经历）也会导致人们产生趋同的语言习惯；根据这项研究，可以将两个身份的写作风格联系起来，并挖掘到背后人的真实身份。

这也是为什么我们在多重身份角色的相关安防建议中强调：您必须能妥善管理每一种身份角色，切勿令它们之间、尤其是这些角色与您的真实身份之间，产生任何联系。

OxyMonster 的多重在线角色之所以被联系在一起并被揭露，是因为“单词和标点符号的使用有很多相似之处”—— 见起诉书：

[image] *United States of America vs Gal Vallerius*

人们在语言习惯上经常会犯同样的错误，这些微妙的细节都可以变得瞄准你的黑枪。

除此之外，手动检查每个帖子的内容，以便与以前找到的照片、社交媒体帖子、和其他信息，建立另一种联系。

Med3l1n 案的另一个证据是，政府间谍在社交媒体背景中找到了一本书“ Gomorra” 的照片，并在华尔街市场论坛上找到了对该书的引用。

[image]

提及其他用户的帖子也会引起调查人员的兴趣，因为这样的帖子会创建目标与之交互的关系网络。

被发现的相关联人可能是目标人现实生活中的朋友、虚拟世界中的朋友、或其他分身帐户 —— 他们的安全操作水平有可能很糟糕。

[image]
[image]

再次强调：您必需与熟悉安全知识并具有良好安全操作习惯的人交往，否则您的朋友会害了您。并且，在分身状态下，切勿使任何分身角色之间产生联系。

时间戳

请注意，信息不足也同样是一种信息！有时也很有价值。

您在社交媒体上的活动已被记录在案，如果政府间谍以任何线索对你产生怀疑，你就会受到重点监视。

强有力的指示器是时间戳，它显示用户何时以任何方式活动、张贴照片、发表评论、或与他人互动。人们一上线就总是想要“做点什么”，

其实这个下意识挺糟糕的（悄无声息真的很难吗？）。

这里再次使用 Med3l1n 的案例作为社交媒体活动和暗网角色如何产生关联的调查示例：

[image]

进行这种调查的任何人都需要考虑时区。

其他指标比如，搜索时使用的语种，如果与其搜索内容本身的相关性很低，那么该语种就很有可能是目标人的原籍国。

建议您不要告诉任何人你住在哪里、在哪里工作，以及你的时区是什么，否则会非常危险！就算是你最信任的人也一样，因为他们有可能扛不住社交工程的诱导而把你说出去。

[image] *Snippet from Med3l1n case*

其他

在暗网上引起间谍注意的任何人都应该明白，你的用户名已存在于监视数据库中，并且每次被提及 —— 不论在虚拟世界还是在现实生活中，都会引起对其的跟踪监视。

[image] *United States vs David Burchard*

当然，这不是决定性的证据，仅是整个案件的支持线索之一，包括物流包裹的拦截、人身监视、或移动跟踪记录等等，都是常用的；但社交媒体情报而不是其他在整个追踪调查中起着至关重要的作用。

所以，今天推荐的这个技术是专门针对社交媒体情报的 —— 也就是一切调查的根基。

这里需要解决的问题是：如何比较来自不同社交媒体的用户；此外，如何比较他们的活动、个人资料图片、语言使用习惯和社区，从而挖

掘他们的真实身份。

[image]

SocialPath

查看与个人相关的所有帖子、推文或照片是繁琐且耗时的工作，手动做会很辛苦 …… 幸运的是，相关自动化的便捷工具其实很多。

SocialPath 是一款简单的应用程序，可在社交媒体（Facebook、Instagram、Twitter、Reddit、和 Stackoverflow）中查找帐户。

它使用 Django 作为后端，并使用 D3js 绘制图表；并提供有关个人资料的基本信息，例如 简介、网址、关注者或朋友。

详细信息页面包含基于用户活动的图表，即 热图日历、lollipop图表、滚动图和 wordcloud。它用于显示用户时间轴、主题标签、词频、提及、评论、以及更多能揭露帐户类型的信息。

键入用户名时，您将使用先前的帐户重定向到仪表板。几分钟后，当字段开始填充时，您将能够看到个人资料图片和主要信息。

[image] *SocialPath Dashboard*

当用户存在时，您可以单击其照片并转到详细信息页面。如果用户不存在，您将看到与您指定的目标帐户相似的其他帐户 —— 因为目标人有可能采取变体名。

[image]

完整数据包括每个现有用户的上述交互式图表。

Heatmap 日历显示用户何时进行互动（例如发布照片或推文）以及执行了多少次。单击每个活动的方块将您重定向到该特定日期的互动上。

[image] *SocialPath timeline of @the_wojciech*

Lolipop 图表显示 Twitter、Facebook 和 Instagram 的主题标签，Stackoverflow 的标签和 Reddit 的 subreddits。

它显示目标人使用了多少次某个固定的标签，以及目标人在特定标签或 subreddit 中处于活动状态的次数。

[image] *SocialPath lolipop chart for hashtags*

滚动条可以帮助您调整特定单词出现的频率，一个人经常使用很多单词，有时某些词只使用一次，因此很难想象出来。但是，它显示了500个在评论、发推、回复等地方使用率最高的词及其频率。

[image] *Words frequency chart*

Wordclouds 用于呈现各种用户交互。例如，对于 Reddit，它会显示点赞，因此可以轻松查看其中有具体点赞的特定帖子。

这是一种确定用户是否受到社区喜欢以及哪种帖子获得最多或最少支持的快速方法。

单击特定编号后，它将重定向您到相关的帖子或评论。

[image] *Upvotes for Reddit user.*

局限性

该应用使用API，因此您需要在配置文件中填写API密钥。根据 Facebook 的政策，仅下载帖子您不需要任何API访问权限。

另外，如果每天少于300个查询请求，Stackoverflow 不需要您做身份验证。

Instagram 允许抓取其公共API，但有时可能需要传递您的cookie，如果您在将 Instagram cookie 复制到配置文件时遇到问题的话。

下面是管理界面：

[image]

在这里看到 SocialPath：https://github.com/woj-ciech/SocialPath

结论

处于显而易见的原因，这里不会演示任何真实的调查过程。您可以自己实践。

如上所述，如果您使用互联网，就必须能做到：

- 切勿将不同平台上的身份信息发生关联 —— 不论是名字、照片、语言习惯、还是兴趣偏好或简介；
- 暗网是相对安全的，但暗网也是警察间谍的重点监视目标（他们的逻辑很傻逼，他们认为“你如果不想鼓捣什么猫腻就不会想使用暗网”）；所以，操作安全是一切的基础，不要犯低端错误；
- 在线分身是非常必要的，其关键在于每一种分离角色之间都不可以有任何相关性！必须不能有其他人知道那是您的分身。

至少 SocialPath 表明，任何人都可以轻松创建此类挖掘社交媒体情报的应用程序，因此你必须假定，政府间谍可以拥有更为强大的情报挖掘工具、实时监控能力、以及更大的数据库 —— 包括来自先前被抢占市场的转储。

要小心。

[image]
[image]

一次性手机用户指南：关于刻录机电话您应该知道的重要原则

[image] 关键词	一次性手机 移动设备
[image] 关联	[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08 ；[image]匿名手机
[image] 创建时间	2022年4月20日
[image] **Description**	操作安全性；行动安全性

并不是设备在保护您的安全，真正能保护您的是人 -- 是人对操作安全性的遵守。

- Table of Contents

  1、刻录机电话与寻常所说的“一次性手机”不完全一样。
  2、您的刻录机电话 只能 与其他刻录机电话通话。
  3、永远 不要在您的家里打开 刻录机电话！
  4、永远 不要在您的常用手机附近打开 您的刻录机电话！
  5、通信时永远不要提及自己或任何联系人的 名字 。
  6、谨防黄貂鱼（**IMSI**捕手）。
  7、刻录机电话必须是一次性使用的。
  8、购买刻录机电话时应该非常小心。
  9、千万不要认为刻录机电话是“绝对安全的”或“绝对可靠的”。

[image]

近期新闻：据《华尔街日报》报道，美国奥运会和残奥会委员会正在告诉运动员们，在参加中国的冬奥会之前放弃他们的个人手机，改用

刻录机电话。

据报道，该公告去年曾两次发出，警告运动员在中国时可能受到数字监控。公告指出："每台设备、通信、交易和在线活动都可能被监控。你的设备也可能被恶意软件破坏，这可能对未来的使用产生负面影响"。该报道指出，英国、加拿大和荷兰也提醒运动员不要将他们的个人电子设备带入中国。

委员会的担心并不是没有根据的。2019年，中国被发现在从新疆地区入境的游客的手机上秘密安装间谍软件。加拿大公民实验室发现，中国的**My2022**奥运会应用程序（所有与会者都必须安装）充满了安全漏洞，可能导致隐私泄露、监控和黑客攻击。

早在北京举行2008年夏季奥运会时，美国国土安全部就向前往中国的任何旅行者发出了类似的警告，警告说携带任何电子设备都有可能面临"犯罪分子或外国政府人员未经授权的访问和数据盗窃"。然而，这次的情况有点不同，由于对COVID-19的担忧，中国已经禁止所有外国观众。运动员们可能会依靠他们的移动设备与朋友和家人保持联系，这可能会在移动数据、短信和通话受限制的一次性手机上更加复杂。

但是，刻录机电话真的就能安全了吗？这是一个重要问题。

[image]

刻录机电话就是一次性使用的电话，与您的身份无关，理论上可以用来在可能被监控的情况下进行匿名通信。如您所知，非常多的行动主义安全性建议中都会提到刻录机电话。

[image]

激进社区用户请从这里进入：[image]匿名手机

以及这里：[image]数字技术限制和最佳实践

但仅仅建议使用，依旧是有问题的。此前我们借助1月6日国会暴动的

大抓捕过程分析了这件事，所有暴徒都在使用一次性手机，但间谍机构依然实现了连锅端，关于他们是如何做到的，见 🔙 https://iyouport.substack.com/p/3ef。

使用一次性手机本身究竟是否是一种“最佳做法”，还有待商榷，但如果您选择使用一次性手机，有几件事您应该牢记。

1、刻录机电话与寻常所说的“一次性手机”不完全一样。

如上所述，刻录机电话是一种专门为匿名通信而采购的、绝对只用一次的手机。它通常被认为是一种私密通信的手段，其功效的前提是要有完美的安全做法！

寻常说的“一次性手机”是指您购买并正常使用的手机（并不强调安全操作），因为您知道它很可能会丢失或损坏。

2、您的刻录机电话 只能 与其他刻录机电话通话。

如果您使用您的刻录机电话与某人日常使用的电话通话，就会打破私密。在您和您的联系人之间留下可追踪的痕迹。

为了您通信圈内每个人的安全，您的刻录机电话应该只用于联系其他刻录机电话，这样您的关系网络就不会危及您的安全。

有很多方法可以安排，但最好的方法可能是记住您自己的号码，并与您希望沟通的人当面分享号码。事先约定让联系人给您发一条非常普遍的短信，这样当您打开手机时，您就可以根据他们发送的信息来识别他们，而不是用其他方法。

如果您是在与一大群人合作，在您的手机开机的情况下完成这个过程可能也是可以的。

在这两种情况下，除非您有非常重要的信息需要传递，否则没有必要回复接收到的信息。也请记住，您应该尽可能少地通信，以尽量减少对您的安全的潜在风险。

3、永远 不要在您的家里打开 刻录机电话！

这是最常见的也是最严重的暴露身份的误操作。

由于手机随时都在记录和传输位置数据，您不应该在任何已知您的身份的地方打开一次性手机。这显然包括您的家，也应该扩展到您的工作场所，您的学校，您经常去的健身房，以及您经常去的任何其他地方。

4、永远 不要在您的常用手机附近打开 您的刻录机电话！

如上所述，手机就是一个带有额外的酷炫功能和特性的跟踪监视设备。正因为如此，您不应该在您的 “真实” 手机附近打开一个刻录机电话。因为这会导致形成一个数据线索 —— 将您表面上匿名的刻录机电话与您的个人身份相关的手机同时放在同一个地方，对于监视者来说就很容易破解您的身份。

这也意味着，除非您在一个很大规模的人群中，否则您不应该在您的重要联系人的常用手机附近打开您的刻录机电话。

5、通信时永远不要提及自己或任何联系人的 名字 。

鉴于使用一次性手机的目的是为了保持您的匿名性和您周围人的匿名性，那就永远不要说出名字和常用昵称/绰号。

通过一次性手机通信时，不要使用任何人的合法姓名，也不要使用您在其他地方使用过的假名。如果您必须使用一个假名，那么这个假名必须是唯一的，是事先确定的，并且只使用那一次，绝不重复使用。

您可以考虑使用一个无害的暗语进行交流，而不是使用任何名字。比如：“嘿，你想在星期二吃早午餐吗？” 而不是 “嘿，我是李大头”。这也允许呼叫和回应作为彼此间的身份认证。例如，如果您的联系人对你的早午餐邀请的回应是：“当然，让我检查一下日程，然后再给你答复”，您就会知道您打算联系的人是正确的人了。

此外，这种认证做法允许使用紧急求救代码 —— 比如 “我不能参加早午餐了，我要去上瑜伽课”，如果您试图协调的人遇到了麻烦，可以使用这个紧急求救代码，收到这样的消息时您就会知道出事了。

[image]

6、谨防黄貂鱼（IMSI捕手）。

必须保持您的身份认证暗语和紧急求救暗语尽可能无害的一个原因是，世界各地的执法机构正越来越多地使用IMSI捕手，也被称为 “黄貂鱼” 或 “基站模拟器”，在其范围内捕捉任何短信和电话。这些设备假装成手机信号塔，拦截并记录您的所有通信，然后将它们传递给真正的手机信号塔，这样您的目标联系人也会收到这些信息。

[image]

激进社区用户请从这里进入：[image]黄貂鱼

正因为如此，您不应该使用刻录机电话发送直言不讳的短信，比如 “嘿，你在抗议活动现场吗？”或者 “你带了燃烧瓶吗？” 这是非常愚蠢的。

在正常情况下，使用 Signal 等加密通信可以相当有效地规避黄貂鱼的威胁，但由于刻录机电话通常不具备加密信息的能力（除非您购买的是刻录机智能手机），因此有必要对您所说的任何话加以编码——变成暗语。

[image]

请注意！使用**Signal** 等加密通信是有规则的，遵守这些规则才能实现安全，否则端对端也无法保护您。具体措施见 BACK [image]如何才能

安全地使用端对端加密（比如Signal）：准则 。

7、刻录机电话必须是一次性使用的。

刻录机电话是为了使用一次，然后被视为“烧毁”。这有很多原因，但主要原因是，避免您的秘密行动相关的线索被联系起来。如果同样的刻录机电话开始出现在同类的反抗行动中，追踪调查这些事件的人就会有更多的数据来建立档案。

这意味着，如果您所做的事真的需要一个一次性手机，那么您所做的事每次都需要一个全新的、安全干净的一次性手机。不要让安全措施的草率执行否定了您的所有努力。

8、购买刻录机电话时应该非常小心。

您的一次性手机应该是不可追踪的。这意味着您应该用现金支付；不要使用任何银行卡。

问问自己：在您购买手机的地方或周围是否有监控摄像头？不要把您的私人电话带到您购买刻录机电话的地方。

考虑步行或骑自行车去购买，不要开车，您的车牌就是您的身份证；用非常朴素的衣服或化妆品遮盖您身上容易被识别的特征（比如明显的痣、疤痕、纹身等细节）；不要在您经常去的任何地方购买刻录机电话，以免工作人员认出您 —— 您永远都想不到有多少人认识您的脸，尽管您从未和他们说过任何一句话。

[image]

激进社区用户请从这里进入：[image]反击, 保持自由：街头实战指南S05E17

以及：[image]从组织到行动：极简战术手册

以及：🎭面部识别

另，⬅BACK [image]S04完美隐身-总章节：机智是重要实力 中介绍了很多隐藏自己的方法，可以参考。

9、千万不要认为刻录机电话是“绝对安全的”或“绝对可靠的”。

为了使刻录机电话能够保护您的隐私，参与通信圈的每个人都必须保持良好的安全文化！

安全地使用刻录机电话要求联系人网络中的每个人都采取适当的预防措施并保持良好的隐私状况：因为一个人的失败会危及你们所有人。

因此，既要确保与您交流的每个人都能在安全和正确使用刻录机电话方面保持一致，也要假设有人可能会粗心大意。这也正是为什么要强调即使在使用一次性电话时也要非常小心通信内容的另一个重要缘由。

始终对自己的安全负责，并在必要时毫不犹豫地删除和丢弃您的一次性手机。

[image]
[image]

一句话安全须知：记住这些句子，以简单地优化您的安全性

[image] 关键词	个人 传输安全 免追踪 加密 反侦察 备份 威胁响应 数字安全 查询整理 清理 电脑 社交网络 移动设备 自助 防御 预防性
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2022年5月18日
[image] **Description**	操作安全性

希望您能把它们当成习惯。操作安全理应成为习惯。

- Table of Contents

匿名化您的在线足迹
1、在抗议活动中
A、关于手机/其他智能设备
B、关于拍照。
C、关于防止自己被识别。
2、在互联网上
A、使用火狐浏览器。
B、一次性账户。
3、如果您觉得自己已经被盯上了。
A、检查自己 **[image]** 自我人肉
B、检查您的信息是否已经被公开
C、从谷歌删除您的旧信息
D、尽可能不要让谷歌跟踪您
E、对于您正在使用的每一项服务，将隐私设置深入到核心部分。
F、删除旧的电子邮件

G、基本安全账户的做法
H、定期删除您的旧内容

[image]

的确有一些基础性的防御步骤，几乎所有人都用得到，也应该被推行。

本文将对此进行一点简要的总结，用最简单的短句来描述您值得考虑的安全习惯。

匿名化您的在线足迹

无论您是亲自参加抗议还是在数字空间工作（或两者都是），隐藏浏览习惯、元数据、和搜索历史，都是很重要的。这些数据可以立刻被作为证据，或者甚至在几个月或几年后暴露您和同伴的身份。

即使没有法院命令或政府的直接监控，您的数据历史也可以从综合性服务中被买到 —— 包括合法的，也包括非法的。

在互联网上，您随时都会被追踪。您走到哪里都会被追踪到哪里，无论是您的ISP、广告商、cookies，还是网站本身。这将是您的IP地址，您大概在世界的什么地方，您在互联网上去过哪些地方，以及通常您持有什么社交媒体账户。

即使只是您使用的浏览器也能告诉别人您是谁，根据所谓的浏览器指纹。由于硬件和软件的组合有限，您可能有一个独特的 “指纹”，仅仅是因为您的电脑设置的特定组合是罕见的。

互联网上的个人隐私一直都在从各个方面被侵蚀，包括广告和商业、薄弱的政府保护、被黑客攻击的数据库、泄露您的信息的产品和服务（通过故意出售信息或“意外”泄露）。但是，互联网从来就不是真正为了匿名而存在的。要使你的信息匿名，需要付出努力。

1、在抗议活动中

A、关于手机/其他智能设备

最好是把您自己的手机留在家里；

警察可以通过手机信号塔追踪手机—— 这可以确认您在“敏感地点”的存在或在以后确认您的身份 BACK [image]移动网络运营商 ；

信息也可以被“[image]黄貂鱼 ”拦截，它冒充信号塔；

如果您使用安卓系统，把它留在家里—— 它有被警察入侵的历史；

如果您有一个旧的/备用的/一次性手机，考虑用它来代替 —— 即使没有SIM卡，只要可以连接到WIFI和蓝牙也没问题 BACK [image]匿名手机 。

如果您确实必需带着自己的手机，想一想您在上面存储了什么，以及所有这些东西是否会使您或您最关心的人处于危险之中 BACK [image]如果您的手机被盗或被警察抢走… ；

根据需要删除联系人和信息。

备份您的数据，以防数据丢失。

关闭主屏幕的通知 —— 在没有解锁手机的情况下，不要让任何东西显示出来。

将您的手机设置为可以极快地进入锁屏状态。

开启飞行模式。

确保 Airdrop 没有开启。

[image]如果您的手机被盗或被警察抢走… ，撤销访问权限并远程注销应用程序；

更改账户的密码有时可以强制注销。

使用 Signal、session、或其他加密的消息系统进行通信。请注意，警察仍然可以监视元数据（关于你什么时候发送信息，通话多久等等），但不能监视加密信息的实际内容。 [image]如何才能安全地使用端对端加密（比如Signal）：准则

关掉定位服务! 这将无法将GPS坐标附加到照片元数据中。

B、关于拍照。

照片可以非常有用，但是，

要在不解锁手机的情况下拍摄照片；

不要拍摄可能被识别出身份的人的照片；

如果您在照片中捕捉到一个人，请将其脸部模糊化或屏蔽掉 [image]在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作 ；

拍完照片后，截图以删除 exif 数据。

Exif 数据存储了图像上的信息，如快门速度、是否使用了闪光灯、日期和时间，以及GPS信息。这可以成为证据—— 不要把照片直接发布

出去，而是截图图片，这样元数据就被覆盖了。

在您对照片进行截图后，删除原始照片。

在没有得到他人明确同意的情况下，不要给他人贴上标签，

也不要在公众可见的空间讨论任何私人计划。

C、关于防止自己被识别。

戴上头巾/面具、太阳镜，遮住任何可识别的特征，特别是纹身和疤痕，包括明显的痣。

不要穿带有可识别标志的衣服，或独特的衣服。坚持使用纯色，或全黑。

最好不要买东西，如果必需买就用现金。信用卡/数字支付都是可以立即被追踪的。

带上可以更换的普通衣服，以便在抗议活动结束后，或者在您必须迅速离开现场时使用。

如果您有能力，可以骑自行车或步行，不要开车—— 车牌阅读器很容易识别您的身份。

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

2、在互联网上

如果您在做研究或在网上活动，不应该被追踪到你，这里有一些掩护自己的方法。

A、使用火狐浏览器。

火狐浏览器增加了追踪拦截和其他数据保护功能，特别是比Chrome浏览器更强。

不要安装任何您不信任的插件，但要安装有助于保护您的数据安全的插件 —— 比如 privacybadger、UblockOrigin。

不使用任何没有隐私声明的软件。

不使用 Dropbox。他们是一家非常反隐私的公司。使用 onionshare 进行文件共享。

不使用谷歌的东西，这里有谷歌服务的替代品。

使用隐身模式。老实说，这并不是一个解决方案，但会混淆一些跟踪。

B、一次性账户。

始终为新账户制作一个没有任何与您有关的信息的新电子邮件。

使用一个假名字。这是合法的，您应该这样做，以避免您的信息数据被跨服务挖掘。

关掉您电脑上的位置共享。

永远不要用信用卡/银行卡支付，最好是现金。

随手删除 cookies 和浏览历史。

关闭 Javascript —— 这是一个无赖，虽然真的很有帮助。

使用 Tor浏览器。Tor通过在世界各地的节点进行路由，使您的流量处于半匿名状态。这是您访问暗网的方式，但您不必去暗网网站，只需使用Tor进行常规浏览。

还有其他浏览器/系统，如 Freenet 和 I2P。

使用代理或VPN（或两者都使用）。代理隐藏您的IP地址，使您看起来像在别的地方，但不对您的数据进行加密。适合于低风险的任务。VPN也使您的IP看起来像来自其他地方，但明显更安全。

更多-> VPN和代理之间的区别。

一些代理。

- https://hidester.com/proxy/
- https://hide.me/en/proxy

您需要确保您的VPN已经过公开审计。

可以试试 Proxygambit ，这是一种简单的匿名设备，它允许您从世界任何地方访问互联网，而无需透露您的真实位置或 IP BACK [image]如何检查您的VPN连接是否实际加密 。

使用一个匿名的操作系统 —— 比如 Tails 或 ZeusGuard，甚至是 Windows To Go。在启动时分配一个随机的DHCP地址。

IronKey 也可以考虑：

一旦您都设置好了，就检查一下是否有DNS泄露：

- https://dnsleaktest.com/
- https://dnsleaktest.com/what-is-a-dns-leak.html

3、如果您觉得自己已经被盯上了。

这种情况下您需要清理您的在线存在，以防身份被盗用/黑客攻击/人肉骚扰/威胁/等。

A、检查自己 [image] 自我人肉

搜索您的旧邮件，翻阅您能想到的每一个曾经使用过的电子邮件；查看那些邮件，以帮助您记起自己可能使用某个邮箱地址注册过的其他网站。

然后，从被遗忘的/不再使用的服务中删除您的账户。

使用每个电子邮件账户的搜索功能，寻找 “注册 Sign up”、“欢迎 Welcome” 等关键字。

恢复并登录到每个服务，清除任何内容和信息，因为一个账户即使在理想的 “受保护” 状态下也可能被归档。

记下您曾经使用过的用户名、密码、服务和使用过的电子邮件地址；然后删除该账户。

如果找不到删除账户的地方，搜索 “删除账户 delete account” ＋“＜

服务的名字＞”。有些时候可能需要给支持部门发电子邮件。

B、检查您的信息是否已经被公开

现在您有了一个用户名、电子邮件和服务的清单了，看看这些是否是任何地方的数据泄露的一部分。

在 Duckduckgo/Google/其他搜索引擎上搜索您自己的电子邮件和账户名称。找找是否有泄露您的信息的数据库或 Pastebin 链接。注意哪些用户名和密码会出现。

要知道，许多数据库没有被搜索引擎收录，于是您应该使用 https://haveibeenpwned.com，检查何时以及您的哪些信息是被公开的。

如果有任何东西显示出来，这将是第一个要改变或删除的优先事项。

C、从谷歌删除您的旧信息

即使您删除了旧账户，也可能有关于它们的缓存信息存在。

使用谷歌控制台，要求他们删除/更新他们的搜索引擎（很不幸这通常需要几个月的时间），以删除这些缓存的结果。您必须提供每个链接。在这里：https://www.google.com/webmasters/tools/removals

D、尽可能不要让谷歌跟踪您

在这里，您可以通过谷歌的每项服务。关掉您的每个账户：https://myaccount.google.com/activitycontrols

您可以在这里看到（和擦除）您的历史活动记录：https://myactivity.google.com/myactivity

您可以在这里报告内容以便合法删除：https://support.google.com/legal/answer/3110420?visit_id=637092788967151292-3839576181&rd=1

E、对于您正在使用的每一项服务，将隐私设置深入到核心部分。

可能的情况会随着服务的变化而变化—— 没有哪个账户是绝对安全的，但一定要尽可能改变设置。

Facebook 尤其糟糕，但如果您想要/需要使用 Facebook，建议确保您的所有信息都被设置为私密，这样至少其他人无法访问您的照片和信息。

F、删除旧的电子邮件

如上，在您浏览了旧电子邮件并找到了曾经注册过的服务之后，您应该删除这些邮件。

这是为了避免留下可能在将来被用来对付您或使您尴尬的个人信息（您可以假定任何时候您都会被入侵、您的设备会被警察抢走或丢失）。

如果您认为自己可能仍然需要这些邮件，请至少确保更改您的安全问题和密码。

G、基本安全账户的做法

定期更改您的所有密码，至少一年几次。要知道，每天都有新的数据泄露和被出售。

切勿使用相同的密码、相似的密码，或在密码中使用个人信息（生日、车牌、门牌号、宠物等等）。

有一些程序可以自动运行密码的排列组合。当然，一个适合您的密码管理器将是最方便的。

H、定期删除您的旧内容

删除推文和旧照片。如果您是被针对的个人目标，这些信息可能会被恶意者集中研究。

要小心发布有关您的社交圈和在您身边的人的任何信息。即使您自己有严格的安全措施和习惯，也您的邻居和朋友可能并没有那些措施—— 如果黑客知道谁是您的邻居，也同时知道了您住在哪里。

好啦，就是这样。记住这些句子对您的基本安全性有好处。

激进社区用户请从 自卫措施 进入；团队和社群的入门培训工作请从S01开始 [image]S01整体安全 - 总章节：前线安防入门课 。

[image]
[image]

Telegram的隐私保护指南，和信息搜索工具

[image]	关键词	telegram 反侦察 开源情报 端对端加密
[image]	关联	[image]数字技术限制和最佳实践
[image]	创建时间	2022年11月29日
[image]	**Description**	操作安全性

搬家真的好难是吧，在数字世界搬家可能意味着关系结构、信息资源和影响力的多方面损失。

如您所知有很多比Telegram更安全的IM，但我们理解大家为什么留在Telegram。

做个权衡吧，把代价控制在可接受范围内。

- Table of Contents
Telegram存在的隐私问题包括：
1、手机号
2、加密
3、云
4、频道
5、加密协议
Telegram的隐私提示
1、位置隐私 ——
2、电话号码隐私 ——
3、在线状态隐私 ——

4、头像照片隐私 ——
5、通话隐私 ——
6、消息隐私 ——
7、群组添加隐私 ——
8、双因素身份验证 ——
9、额外的安全——
针对Telegram的信息搜索工具
以下是一些 Telegram 的搜索引擎

[image]

我们一直都不推荐 Telegram 作为敏感通信工具，它的唯一优点只有频道。但也因此，它汇聚了全球消息来源，尤其是对于突发事件来说，于是吸引了极大的人气。

我们此前介绍了 Telegram 用户被去匿名化的方法，见 https://www.patreon.com/posts/cong-telegram-lu-72200795 ；本文将首先简单梳理 Telegram 的隐私安全问题，如果您必需使用它，至少应该注意这些事。

Telegram存在的隐私问题包括：

1、手机号

电话号码和其他与Telegram账户相关的数据都会被定期收集和储存，这对SIM卡实名的国家用户来说相当不方便（所有强制手机号码注册或验证的应用和服务都不值得推荐）。

此外，当您的联系人之一加入该应用时，您就会收到通知（其他所有在Telegram上并且联系人中有新加入者的人也都会收到通知）。

2、加密

标准的 Telegram 聊天并不是端对端加密的，要使用加密您必需手动选择。

telegram 群组也不加密，甚至可以通过搜索引擎找到。

3、云

Telegram 只对传输中的数据进行加密（在服务器和终端用户之间），但它不对静态数据进行加密—— 已经发送的信息未加密地存储在Telegram的云服务器上，理论上Telegram的员工可以随意访问所有这些信息，或者在数据泄露的情况下被无意中作为纯文本发布。

这也是此前那位俄罗斯姑娘被抓住的可能原因之一。

4、频道

如上，**Telegram** 上的群组和频道也是如此，无论它们是公开还是非公开的。在那里分享的任何东西，包括文件、多媒体等，都没有真正的隐私。

5、加密协议

在对内容进行加密时，Telegram使用的是 MTProto，这是它自己的加密协议，也就是说没有其他人使用。虽然到目前为止还没有任何令人担忧的报道（MTProto毕竟是开源的），但这有可能成为问题，因为众所周知，专有的/晦涩的协议中的安全缺陷比被广泛使用的协议更难被发现。

如果您不得不使用 **Telegram** 并且担心自己的人身安全和隐私人权，唯一方法是为一对一的交流启用端对端加密。群聊就算了吧，真的不推荐。

请注意，端对端加密的聊天只能在移动设备中进行，不支持桌面版。

[image]

您可以在本站的“工具-Tools ”专题中搜索“IMs”，查找可能适合您的安全通信工具。

Telegram的隐私提示

建议所有中国用户务必做到以下这些措施中至少90%；敏感用户建议做到100%。

Telegram多年来都是中国当局的重点盯防目标之一，您可能也知道这件事。

1、位置隐私 ——

确保 “附近的人” 功能被关闭（进入 “联系人” > “查找附近的人”）。这项功能应该是默认关闭的，除非您出于某种原因将其打开了，不要打开。不要用它来找朋友！

在抗议现场的人们建议使用 **Briar** 或 **Berty** 等。在这里看到更多。（理想状况应该是您在自己的团队中提前部署这些设施；最差的情况是在抗议现场紧急组织并部署这些设施，以绕开镇压者的渗透。）

[image]

返回：[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训

返回：[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

2、电话号码隐私 ——

进入Telegram设置 > 隐私和安全 > 电话号码。在那里，关于谁可以看到您的电话号码 > 选择 Nobody。不论您注册用的号码是否实名，都建议选择隐藏。

3、在线状态隐私 ——

转到 Telegram 设置 > 隐私和安全 > "最后出现&在线"，在这里选择 Nobody。

这可以让您对其他用户显示为永久离线。

（这点很重要，加密货币爱好者可能更了解这一安全措施？如果您尚未了解并且感兴趣，我们可以在未来更详细解释。总之，这里先选 Nobody。）

4、头像照片隐私 ——

进入Telegram设置 > 隐私和安全 > 头像照片。在那里，选择 "我的联系人"（很遗憾这个地方您无法选择对所有人隐藏，所以，请特别注意不要随便添加联系人！确保只添加您认识的人！在这里看到伪装您的熟人这种手段如何成为对您去匿名化的攻击形式）。

5、通话隐私 ——

进入Telegram设置 > 隐私和安全 > 通话。在那里，选择 **Nobody**。

6、消息隐私 ——

进入Telegram设置 ＞ 隐私和安全 ＞ 转发的消息。在那里，选择 **Nobody** （注意，在下面您可以添加个别例外。尽可能不添加比较好）。

7、群组添加隐私 ——

进入Telegram设置 ＞ 隐私和安全 ＞ 群组和频道。从那里，选择 “我的联系人”。这将防止随机用户将您加入群组和频道。

8、双因素身份验证 ——

进入Telegram设置 ＞ 隐私和安全 ＞ 开启2FA。

9、额外的安全——

对于那些有额外安全意识和/或需求的人来说，以下两个额外的功能可以利用：

a) 禁用数据和存储设置中的后台下载选项 **Background Download** —— 这将阻止应用程序自动下载媒体文件，让您可以更好地控制您想下载什么文件以及从谁那里下载。

b) 启用链接预览设置 —— 进入Telegram设置 ＞ 隐私和安全 Privacy and Security ＞ 数据设置 Data Settings ＞ 链接预览 Link Previews。这将允许您在点击链接之前进行预览，以便减少钓鱼攻击的可能性 —— 建议拒绝所有缩短链接！在查看到原链接之前不要直接点击！查看原链接的方法在这里。

针对Telegram的信息搜索工具

昨天我们提醒了接下来更可能出现的局势 —— 不仅有“秋后”，还包

括信息战，统治者将使用大量歪曲的信息污染抗议战略，分化抗议者、恐吓支持者，旨在扑灭那些已经燃起的火焰。

这种情况下后勤人员需要发挥作用：搜集信息、验证信息，即 开源情报。准确说是社交媒体情报。我们发布过非常多开源情报工具集（有一整个系列）但现在您可以不容易找到最想要的工具。于是以下内容我们将总结一些针对 Telegram进行搜索的基本工具。

强调，建议参与这项工作的朋友为 Telegram 安装一个桌面应用程序，这里是下载页面的官方链接，这样可以简化搜索，并允许您绕开移动应用环境的限制对URL进行操作。

聊天记录导出功能也只限于Telegram的桌面版。可以通过在桌面应用程序上打开感兴趣的聊天，并点击右上角的三点图标来找到它。您可以选择您的聊天记录导出偏好—— 以及选择下载文件的大小限制（目前最大为4GB）。

以下是一些 Telegram 的搜索引擎

Commentgram—谷歌为Telegram频道中的评论定制的搜索引擎。

Lyzem—被宣传为“专门为Telegram和Telegraph平台创建的独立搜索引擎”。是搜索关键词、频道和公开组的可靠工具。包含一个允许用户对帖子进行索引的综合服务—@IndexPost_bot。

Telegago—专为Telegram的谷歌定制搜索引擎。

Telemetrio—按评级、人气、国家等排序的Telegram频道的巨大列表。

TGStat—包含大量的可搜索目录和特定国家的频道指标。

Tlgrm EU—按类别分组的各种频道列表。这个网站维护着一个频道目录，如果您有自己喜欢的频道，可以通过填写一个小表格后将您的最爱加入该目录。

还有其他 Telegram CSE，很多开源情报爱好者都在开发自己的小工具，搜索结果可能有所不同，取决于它们索引的来源，也取决于这些来源的更新程度。比如这里是一个可靠的 Telegram CSE 的例子（作者不详）。

就是这样！希望所有抗议行动的参与者和支持者都能顺利平安。

[image]
[image]

当您准备像编程随想那样工作...：须知

[image] 关键词	个人 反追踪 威胁响应 威胁模型 数字足迹 整体安全 防御
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2023年3月27日
[image] **Description**	操作安全性

安全问题不是纯粹的技术问题。对安全的普遍误解导致了很多难以被察觉的安全漏洞。这些漏洞可能没有简单的 "补丁"。

- Table of Contents

  关于最普遍的安全漏洞
  —— 第1个弱点：对对手的了解不足 ——
  —— 第2个弱点：孤独 ——
  第1步
  第2步
  第3步
  第4步
  此案评论中显示出人们对 “安全” 可能存在的误会
  1
  2
  3
  4
  最后

【注】如果文中导图看不清楚，请右键选择 “新建标签页打开”。或者，您可以在这里下载。

[image]

失踪已久的前著名华语博主“编程随想”，于近日终于有了比较确切的消息—— 正如很多人所担心的那样，失踪意味着发生了糟糕的事，他被捕了，而且还被判了刑。

[image]

如果此时有任何人感觉到自己的头脑中充满了安全性虚无主义的噪音，请不要自责，这是正常的。“专家都被抓到了，我等菜鸟还能幻想什么”……

但这样想至少毫无作用。

因为，安全问题不是纯粹的技术问题，就如安全这个词本身所描述的东西一样，它是一个系统，一种状态；于是它的结果取决于协调性，而非其中某个/或某几个部分的专业性。

同时，不幸的是，局部的专业性过高有可能降低（而不是提升）整体的协调性。

[image]

本文不是文章，只是一个帖子。它可能非常不完整（毕竟没有卷宗可查）；但也许可以补充一些编程随想博客可能没有涉及的内容。此外我们也正在准备一本书，希望能更详细地讲述安全这个问题。

在收到起诉书全文之前，我们发布了一个帖子如下。大概需要解释一下：起诉书只能确认判决事件，但起诉书中所描述的侦查细节，建议谨慎取信。对刑侦过程/手段的调查，是另一项任务 —— 是更重要的任务，对所有政治犯的案件来说都是如此，不论当事人最终有没有被起诉。

[image]

关于最普遍的安全漏洞

在安全方面，中国的前线工作者有两个方面的弱点，比较严重。

—— 第1个弱点：对对手的了解不足 ——

您肯定知道 “知己知彼” 这一重要的战术智慧。您的对手拥有巨大的特权、充足的预算、无下限的卑劣，以做到长期、持续、深入地了解您，甚至可以预测您的行为。而您对他们了解多少呢？

这里存在一个严重的不平衡。您在明，他们在暗。

缺少的可能不是吹哨和调查，而是满足前线社区反抗战略的战术。这至关重要。

我们对此的弥补方案，是努力分析其他国家的镇压手段（内容在 列表-5 “中：https://start.me/w/65mjN4 和 https://start.me/w/5ax6G0 ）。鉴于统治者所拥有的基础设施大同小异，这可以有所帮助，但肯定不充分，前线工作者需要了解对手在什么样的情况下倾向于怎么做。

[image]

如此，您便既可以 “制造” 某种情况，以引诱对手那样去做，

也可以避免某种情况的发生，以改变事态走向；

甚至还有可能从中了解到对手可能的漏洞，以利用来维护自己的安全。

在其他很多国家，反对派组织是很擅长做这类事的，他们在努力保护自己的秘密的同时，揭开对手的秘密。这也正是 “较量” 这个词所描述的意思。

举个例子：您知道自己在什么情况下会被监视锁定吗？—— 我指的是

刑侦中的监视工作，您知道被锁定的人会经历什么吗？监视者的目的是什么？他们的工作流程是什么？……

我来画个图，以最简化的方法描述俄罗斯镇压机构是如何做这件事的。在您的国家它应该大同小异：

[image]

您能画一个中国版吗？

不必画给我。只给那些与您实际合作的亲密队友。知情对你们来说至关重要。

以上只是一个例子。您需要知道的东西挺多的。请保持战略目标的清晰。

—— 第2个弱点：孤独 ——

孤独是巨大的安全隐患。

令您深陷孤立无援的恐慌，是您的对手始终致力于采取的镇压策略。

人们被渗透和出卖的故事吓坏了。很多担忧是有道理的，但仅仅担忧就没有道理了，因为它只会起到反作用。当您草木皆兵加倍孤单的时候，就是您的对手可以对您最随心所欲的时候。

[image]

激进社区用户请从这里进入：[image]反渗透/线人&减轻背叛的损失 - 总章节：止损于未病

您需要至少一位贴心战友 —— 更好的是 亲密团队。

阮先生的案件之所以变得 “疑点重重”，甚至一大群人因为猜想而发生

争执，正是因为阮先生对紧急状况的准备似乎严重不足 —— 这绝不是额外的工作，它就是“安全”工作本身的重要部分！

这一“准备”工作应该至少包括以下**4**个步骤：

1. 明确威胁环境；
1. 明确您最需要的帮助；
1. 确定至少一位贴心战友 —— 作为紧急联络人，至关重要！
1. 准备具体的材料。

下面的图片分别解释了这4个步骤包括什么：

第1步

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

第2步

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

第3步

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

第4步

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

上述这4个步骤是您 最基本应该做的 ！甚至，不论您是否如阮先生那样去工作，只要您生活在警察国家，并认为自己有遭受迫害的可能性，您就应该提前做这些训练和准备工作。

此案评论中显示出人们对 “安全” 可能存在的误会

1

我们提供过很多安全教程，试图从各方面讲述安全性；这些 “方面” 彼此嵌套，或互为条件，或互相支撑。并没有谁比谁更重要，但它们在不同计划/项目中、在不同程度上，缺一不可。

[image]

安全是一套思考方式。它既不是哪些软硬件、也不是某些配置，

因为没有任何软硬件和配置能独自决定安全性 —— 它们都只是战术，

而安全是这些战术经过有效部署以恰当的方式结合在一起时，所产生的效果。

反过来说，如果它们的组合不恰当，不论是过度还是不足，都会形成安全漏洞。

阮先生的起诉书中出现的细节—— 比如小米手机、华为笔记本等等 —— 也许会让一些读者觉得 “抓住了要点”，其实所有这些都可能不是要点。

这并不意味着鼓励您去购买哪款手机或电脑；什么对您好什么不好，

始终取决于您准备做什么，以什么角色来做。

还有诸如 [image]一句话安全须知：记住这些句子，以简单地优化您的安全性 这样的 “通用” 安全性教程，但防御工作是一个整体，绝对没有那么简单。不幸的是，大多数人可能对软硬件评测头头是道，对配置如数家珍，但却不擅长或经常忘记评估恰当性。

工具很重要，没错，它们提供“能力”给您。但这份能力用来做什么，如何搭配这些不同的能力，取决于您合理的战术布局。

[image]

合理的战术布局 ＝ 有一个明确的战略目标 ＋ 准确的威胁模型和风险评估 ＋ 了解不同战术的特征和能力。

所以，如果您关心安全知识，并且现在是第一次阅读IYP的内容，推荐您从本站的S01教程开始。该训练可以帮您培养一种持续稳定的敏锐，帮助您及时规避风险。

安全就像一棵树，软硬件是小树枝和树叶，而根基是您的战略智慧。

“最好的” ＝ 最合理的和最恰当的，绝对不是 “最贵的和最麻烦的”。

安全就像鞋子，好不好取决于是否合脚，而不是它看起来有多漂亮、花了多少钱、或者有多复杂。

一般情况下人们习惯于假设讲述数字安全知识的人最擅长数字安全操作。也许是这样。但一个人在现实中具体如何操作，起决定性作用的肯定不只有他/她的知识，更多是他/她那一刻的心理状况、情绪状态、经济状况，以及其他很多外部条件。

[image]

再来分别看这三个部分：

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，

以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

近日还传出疑似中国的威胁行为者利用虚拟机的零日漏洞的报告。社交媒体上有用户将此消息关联到阮先生的被捕事件上，怀疑他被恶意软件击中了。

的确，全球大国都在囤积零日漏洞；这是21世纪最危险的武器。但您是否会遭遇零日武器，始终取决于您的角色和您的具体工作 —— 即，您最可能面对什么样的威胁者，61398部队与公安部和国安部，是肯定不同的。请记得，您的对手的武器库中“有什么”，只是一方面，更重要的另一方面是，您的对手是等级森严的官僚机构，他们采取什么做法是有标准的和需要上级批准的。（虽然如今“私人镇压雇佣兵公司”之类的东西也开始出现，值得警惕。因为这些人是流氓，几乎没有约束。）

对于虚拟机零日来说，作为异议人士您不必太过担心。因为，首先，您不应该完全彻底地信任任何一款软件能百分百安全 —— 不论是Tor还是qubes OS还是其他虚拟机。漏洞是政治性的，而不只是技术问题，这就是为什么它永远都“补”不完。其次，隔离风险的第一层屏障，应该在您的头脑中，而不是在虚拟机里 —— 您应该培养一种安全性直觉，将安全操作纳入习惯 —— 就像饭前洗手那样，不需要特意的记忆，也会主动去做，主动拒绝无法完全信任的信息。

如果您只是专注于国家级APT组织的最新能力，就有可能陷入安全性虚无主义。那是没有必要的。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

阮先生的文章中提供的安全建议大多是结论。对于安全知识的初学者来说，这有可能造成一些误会，认为只要完全照着做就行了。并不是的。如果您在阅读后没有进行分析，那对于阮先生的工作来说是一种浪费。

分身只是把敏感的那部分隔离出去就行了吗？当然不是。

如果就像目前公开的消息所言，阮先生的真实身份就是网络安全工程师，那么“编程随想”这个身份就没有实现真正的分身隔离；因为——分身的要诀在于，分离出来的每一种身份之间都是完全不同的，尤其是，没·有·任·何·交·集，必须让每一个身份看起来·完·全·独·立，这样才能切断追踪线索。

阮先生在数字安全方面下了很多功夫，很专业。但战术布局规划方面的技巧至少在博文中的体现不多。

准确评估风险、并掌握安全使用各种类型的在线身份所需的技术技能，至关重要。

关于战术布局，我们以在线身份管理为例，演示下应该建议您如何思考——

在观看下图之前，希望您的头脑中已经有了一个关于您马上准备去做什么的尽可能具体的想法，这样您可以更有代入感，更容易举一反三地使用它来为自己的安全部署进行计划。如果您还没有任何想法，那么可以把自己想象成阮先生：

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

就像所有的安全和隐私策略及工具一样，当您没有面临直接的威胁时，您会更好地学习熟练使用这些防御措施。压力会影响您参与风险分析、安全规划和技能培养的系统化过程的能力。

所以，把安全措施作为习惯，而不是救急，才最有希望获得安全。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，

以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

[image]

您的战术布局应该致力于减轻/减缓脆弱性、增加复原力，而不是寻找 “完全避免风险” 的方案。并没有那样的方案。

减轻/减缓脆弱性的方法，比如，一个分身只做一两件事；完成后彻底摧毁。以及，您不可能完全避免风险，但您可以分散风险/分散敌方火力...... 您知道该怎么做。

还有更多。我想留给您去思考。这些是阮先生可能没有留给您的。

3

完整的 “安全” 措施，必须包含充分的自我评估，和假设所有防御都失败时的**Plan B**。这也是阮先生可能没有做到的。

所有灾难都不是瞬间的突发 —— 威胁在一步步逼近，或长或短，但肯定有一个过程。而最终，这场灾难是否对您产生破坏性、多大的破坏性，取决于您是否及时察觉到步步逼近的威胁，以及您的反应是否机智。我们称之为 “态势感知”。

（此处建议您回顾上文中描述FSB刑侦流程的那张图）

阮先生如果对自身的评估足够准确，并对环境事态足够敏锐，他应该能察觉到威胁，并准备好 Plan B。如果他这样做了，现在的一切胡乱猜测都将不会存在。

自我评估是确立最恰当的防御设施的基础，您应该尽可能准确地描述自身能力和脆弱性：

- 能力 ＝ 有助于使您更安全地抵御特定的威胁的因素（即 降低其可能性或影响）

- 脆弱性 ＝ 会使您更容易受到威胁（即 增加了威胁的可能性或影响）

这里有一个公式，您需要记住：

[image]

风险 ＝ 威胁 ×弱势 ÷ 能力

威胁指的是您的对手所采取的任何手段以试图让您相信他们将不惜一切代价阻止您。

弱势指的是，您知道在那些威胁面前，您自身有哪些弱点（这是需要弥补的部分）。

[image]

值得指出的是，可能与很多朋友的认识相反，使用假名或者匿名工作在这里应该被列为 “弱势”，而不是“能力”。

因为，首先，假名或匿名意味着，人们知道您做的那些事，但不知道您的名字和身份，于是当局就有可能趁机栽赃给您的真实身份以其他罪名，而否认您是因政治原因而遭受迫害。

其次，如果您没有隶属于一个强大的组织，在您被强迫失踪的情况下，营救的希望将非常渺茫。

这就是为什么您必须有 **PlanB** 和紧急措施！匿名工作者孤军奋战是不可取的！

具体做法见全文中的导图 —— 那**4**个步骤。

为了使用上面这个公式，我们先来确定几个定义：风险、威胁、能力、弱势。

1、风险—— 指发生伤害事件的可能性；

2、威胁—— 有意图对您造成损伤、处罚或者伤害的声明或者迹象（近期的或当即的）；

3、能力—— 可提高安全保障的任何资源（包括自身能力、人脉关系、可用的环境条件等）；

4、弱势—— 很可能直接造成或导致更大伤害的一切因素。

这里的施害者可能包括：政府、警察、间谍机构、大公司、利益集团的雇佣打手、极端保守派社区、严重误解您的事业和偏好的家属/父母，等等。

下面我来演示一下这件事该怎么做。以阮先生为例，请注意，目前为止我们对阮先生的现实生活依然一无所知，于是下图只演示这一评估的思考框架，其中所标注的具体事项完全是猜测的，它们只为体现做法，并非分析。

这一框架非常简单，只有4个部分，但是，您必须保持足够的谦逊和诚实，尽可能清晰且详细地描述，才能帮您制定更准确的防御策略：

先看右侧

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

再看左侧

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

措施

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

4

难度越大、越复杂，防御效果越好吗？绝对不是。

并不是说复杂的技术有任何问题 —— 请不要仅仅从技术逻辑上考虑 —— 复杂繁琐的解决方案不应该作为首选是因为，它们会让您难以长时间坚持住，您稍微一疲劳，就可能出错。在安全问题上，您出错的机会很可能只有一次。尤其是在您已经被镇压当局视为一个 “肥美多汁的大鱼” 的情况下。

真正的安全效果出现在您游刃有余的情况下。闭着眼就能做对的情况下。所以，它必须足够简单，需要特别记忆的东西越少越好！

曾经有读者询问如何追踪加密货币（我们介绍过相关知识），以测试隐私程度。但必须说，加密货币安全性是一个更为复杂的领域，在基本数字安全基础之上还有很多额外的知识。马上学是来不及的。如果您不擅长这个领域，那就不要在最重要的/或者可能最危险的工作上选择加密货币。

[image]

换句话说，建议选取您容易上手的解决方案，而不是紧急学习新的复杂的技能。因为熟练操作，是最基本的安全保障。

当然肯定要鼓励您学习新的更好的技能，但是，要在您感觉安全的环境中、在您没有压力的情况下，慢慢学习，而不是在火烧眉毛的情况下临时照着教程画虎。

必须承认，数字技术有点门槛。很多需求者对网络上形形色色的安全建议的态度比较盲目，很难自行判断它们的恰当性和准确性。于是搜索排名就变得更危险了。这更需要安全建议提供者保持诚实！拿钱写

软文的人，如果您觉得自己必须做这行，那么就去写一些牙膏袜子的软文吧，请不要涉及药品和软硬件，这是有可能危及生命的领域。

不论您是否擅长数字技术，建议您记得这个基本原理：少即是多。您下载的东西越少，您的攻击面就越小。完全没有必要把其他人推荐的 “好东西” 全装上，那样做只能是累赘，反而令您更危险。

再一次强调，对抗性思考方式至关重要！反追踪的最好方法就是，用追踪者的思考方式来检查自己。

最后

本案引起的所有猜想都是不必要的，不论其有没有或提供了多少证据。

它最初是一个强迫失踪案件，之后是一个政治审查案件。对于强迫失踪，这在全世界都是难题 —— 最终判刑的结果已经是其中 “最好的” 一种了，更糟的和并不罕见的是：暗杀。这就是为什么需要不断强调联合和互助，绝不鼓励单枪匹马。尤其是当您匿名工作时，单枪匹马是致命的！

看到一些读者在交流此事时倾向于认为警方 “抓错人了”。希望真正的博主没有被捕的那种心情可以理解，但是这会起到反作用 —— 它相当于承认 “对的那个人应该被抓”。不，没有任何人应该因发表评论而被判刑。阮先生究竟是不是 “编程随想本人”，没有那么重要，这里重要的是对政治异议言论的入罪。我们认为将此作为辩护方向，将是对 “编程随想本人” 的尊重。

当然，辩护方向由律师掌握，家属意见将作为重要参考，而不是公众舆论。

再一次，我们希望此案能提醒更多人对安全性的重视（而不是虚无主义），对安全作为一个系统的理解，体悟战术布局的智慧，未来更少

出现这类事故。

[image]
[image]

技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

[image] 关键词	个人 加密 去中心化 变革 团队 大规模监视 威胁模型 对抗性思考方式 工具 开源 战略策划 操作安全性 数字安全 数字足迹 监视资本主义 社交网络 自主 自卫 自托管 自检 防御 预防性
[image] 关联	[image]一句话安全须知：记住这些句子，以简单地优化您的安全性；[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？
[image] 创建时间	2025年1月1日
[image] **Description**	操作安全性

我们有一些障碍需要克服，包括自身的、也包括系统性的，资源垄断可能是最为深层的灾难之源。但不要过于沮丧，我们现在依旧能有一些办法可以减轻危害，关键在于，您必须理解一些重要的问题 ……

- Table of Contents
权衡利弊通常不是很吸引人
第1部分：您的屏幕背后发生了什么？
第2部分：什么有效，什么无效
选择技术工具的一些 有用原则
第3部分：一些基本工具的建议

从设备上管理您的在线通信
对网络浏览器的建议：
推荐的附加组件
电子邮件：
密码管理器：
即时通讯工具：
安全文件存储：
并不是每片云都有一线生机
加密的重要性
总的来说，有些事您需要记住：
在线工具的建议
交流和聊天 ——
语音和视频群组通信 ——
协作 ——
项目管理：
第4部分：缩小范围，进行长期思考
只要您在网上，您就很可能会被追踪
集体问题需要集体行动

[image]

本文将讨论的是，在这个复杂的时代里，如果我们想负责任地远程行动和工作，哪种技术是好的、安全的、适合使用的？如何决定您应该信任哪些技术？以及，未来可以做些什么来使回答这个问题比现在更容易。

权衡利弊通常不是很吸引人

在这个危机时期，全世界正处于技术的十字路口上。人们正面临着看似高效、快捷的技术与看似道德、安全的技术之间的权衡。无论哪种情况，我们都必须处理长期的政治和社会后果 —— 究竟是放弃我们的价值观，还是投资于公平的技术。

每当有事情发生，迫使人们重新思考什么样的技术是可用的，以及应该如何使用它的时候，权利组织都会被问到：推荐什么样的工具是用户友好的、实用的，并且不会危及人们的安全、隐私和保障？也就是说最常用工具的替代品是什么。许多人要求推荐以用户权利和隐私原

则为主要设计选择的沟通、协作和网络工具，尤其是，这些工具在工作时必需不会出现 **Facebook**、**Alphabet** 或类似寡头公司的大数据囤积综合体。

在当前冠状病毒大流行期间，这些问题变得更加频繁。人们的期望是，终极的无懈可击的现成工具箱；人们想要的是他们应该安装的工具清单，他们可能不想去解决为什么要使用这些工具或为什么不使用这些工具的问题，这些问题其实是很难的。情况有急迫性，人们对自己所做的每一步选择都会非常小心，所以我们最终往往会建议一些简单易用的替代方案，这些方案对技能、资源和时间的投入要求较低。但这并不是—— 也不应该是 —— 如此简单。

本文汇编了关于远程协同工作技术的解释、意见和建议。您还会发现很多关于进一步阅读的想法以及在哪里可以找到它。

本文分为四个部分，它需要您花一些时间来阅读，但我们希望它是值得的。

第1部分：您的屏幕背后发生了什么？

[image]

人们经常有这样一种想法，即 有一些工具可以始终为每个人、每个地方工作；不需要额外的知识和额外的基础设施；公平公正，并在任何时候都能保护用户。可惜，这是一个尚未实现的梦想。

我们所掌握的东西离这个梦想还差得很远，非常远—— 20年来，我们已经看到从数据痕迹很少的独立工具到完全为采集尽可能多的个人数据而打造的工具的重大转变；但遗憾的是，今天人们所依赖的大多数工具都还是由那些只具有硅谷思维方式和依靠提取个人数据的商业模式的企业所制造的。

如果您没有时间读祖博夫的《监视资本主义时代》这本书，至少要读

读这篇采访。或者观看下面这个简短的纪录片。顺便说，这本书是有中文版的。

https://youtu.be/hIXhnWUmMvw

我们现在可以有两种方法来处理数据控制和技术选择的问题：一种是缓解，或 “让它不那么糟糕”；比如S02的思路 [image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法 。

我们理解许多个人、团体和组织无法对自己正在使用的技术进行重大或急剧的转变，这可能是由于缺乏资源、技能、知识、帮助或资金。对此的解决方案是满足他们的需求，并在已知的环境中引入渐进式的改变和逐步改进。这种方法也许不能解决根本性问题，但可以减少一些问题。它可以使用户走上正轨，更好地了解技术本身，并建立信心，以便在未来做出更多的选择，采取更雄心勃勃的步骤。

第二种方法是关于思维方式的改变，或者说 “短期痛苦，长期收益”。这一点更难实现，甚至目前为止连谈论它都不够直接。

[image]

“可持续的、安全的、独立的技术“ 需要我们对技术的思维方式有更重大的转变。它需要更多的投资和资源。

尽管我们一直在提倡自由和开源的解决方案和自我托管，但这对许多小型团体和反抗组织来说可能不那么现实。更实际的是，这需要大量的资源：技术可能是免费的，但租用服务器或购买服务器却不能免费；维护它们也不是免费的：您不能依靠志愿者，它需要您不断更新自己的技能和资源。它还需要培训和资金环境：如果您想支持独立、安全、有弹性和可持续发展的组织，就必须像考虑管理、财务或人力资源一样考虑技术。

这些都是工作的基本工具，它们需要认真的长期投资。这种投资不仅要针对用户，也要针对技术制造者。其中一些工具之所以存在可用性问题、设计上的缺陷或陡峭的学习曲线，是因为它们是由资源极其有限的小规模的、专门的团队运行的。

第二种方法不仅需要改变思维方式，还需要系统性的 技术政治的转变。

这两种模式描述了我们现在的处境：要么吃快餐，要么自己种。前者方便，但不是很健康；后者对我们来说更好，但需要耗费时间和技术。

您能用封闭的和专有的工具建立一个民主、公平、开放的社会吗？您是否知道任何一个由公司拥有的公共空间还能运作良好？您是否经历过一个被监控摄像头和传感器封锁的公共空间还能运转良好？

我们现在使用的大多数工具不仅是基于“云”的，而且是为了尽可能的简单（所谓的无摩擦）和吸引尽可能多的用户（所谓社交性），而这些用户又会反过来依赖他们的平台（所谓的基于用户）。这些平台是免费提供的（你就是产品），他们把用户群变成了一个数据库，然后就可以据此赚钱（通过定向广告或类似的方式）。

每当您点击“我同意”，让他们访问您的一切私密行为（元数据），并为 cookies、beacons、脚本和其他什么玩意儿提供所谓的便利 —— 什么都可以，包括浏览器指纹（追踪器），灾难就开始了。一个解决方案是安装一个广告拦截器，但同样的数据也在被用来塑造您的整个体验：过滤气泡、定制机器人、提示、黑暗模式等等。

您对这些技术的体验远不是开放和自由的，它也远不是高质量的。现在人们已经知道了监视资本主义行业的这些事，但人们还是在使用这些工具，因为大家都在用，而且这些工具很容易依赖。

这里值得提出的另一个想法是关于依赖性。这些被数十亿人、公司甚至政府使用的集中式服务的任何崩溃或中断，都会造成同等程度的问题。大规模的依赖性会造成大规模的责任。您已经看到了，当 Facebook/WhatsApp 或 Google Docs 等服务出现短时间故障时，这意味着什么。如果它们瘫痪了几个星期呢？这些工具和其他工具一样 —— 它们有其极限和临界质量。问题是，它们何时会达到它们的极限，以及会带来什么后果。问题早已不在于是否，而在于何时。

最后一个想法是关于漏洞的。像英国这样的国家的首相在家里使用Zoom 这种未经测试、不安全的专有软件来管理政府，这真的是一个好主意吗？这些挑战不仅是对民间社会的挑战。不仅是人权维护者和调查记者需要保密性和可信赖的工具来维护他们的诚信和安全，它同样适用于政府、企业、公共机构和任何个人。

[image]

“无摩擦” 等于毫不费力。但是您必须知道，在现实世界中，摩擦是理解系统和做出选择的必要条件，就像在个人关系中那样。

同样，当我们在技术设计中消除摩擦时，东西变得更容易使用，

但是，我们却失去了认知能力，无法理解它们是如何工作的，

以及它们背后的商业模式是什么。

这种方法，再加上人们互动的 “游戏化”（奖励计划、无尽的滚动、积极的反馈循环），让人们对工具的做法产生依赖，否则人们可能不同意这种剥削的商业模式。Facebook 和剑桥分析公司的丑闻就是一个例子。

[image]

延伸：https://iyouport.substack.com/p/pr?utm_source=publication-search

如果你对这些商业技术解决方案的资金来源感兴趣，可以阅读这里的报告 https://www.newyorker.com/magazine/2020/01/27/is-venture-capital-worth-the-risk

危机，特别是像COVID-19这样的危机，不仅对社会、经济和民主造成了致命的危险，它还为促进和依靠专制的运作模式创造了肥沃的环境 —— 而技术在这里非常方便。

能够进行监控的技术总是以所谓的（国家）安全和保障的名义被推广。这并不是什么新鲜事，在其他类型的危机中或为了应对问题 —— 如所谓的恐怖主义、边境管制、或难民流动—— 全部都使用过。我们已经可以看到，在应对COVID-19危机时，许多相同的技术——如手机地理定位追踪—— 正在被更广泛地侵入性地使用。因为《恐惧诉求是一种最强大的心理操纵工具》。

您可以在这份报告中看到全世界的状况

[image]

延伸：https://iyouport.substack.com/p/lr-covid-1984-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/--f9b?utm_source=publication-search

在这篇文章中，您会发现一些解决方案和相关参考资料 —— 它不是您正在寻找的万能的魔法清单，而是更现实的一种思考技术的方式，可以帮助您做出对自己、您的社区或您的组织有用的、知情的、可验证的选择。

选择是存在的 —— 真正的挑战不仅在于如何做出选择，而且在于我们通过做出选择来支持一个什么样的社会。

第2部分：什么有效，什么无效

[image]

选择技术工具的一些 有用原则

在这里我们将解释一些原则，这些原则一直驱动着人们的选择，我们将提出一些具体的建议。

这里的想法是给您一个框架，帮助您找到合适的解决方案，满足您的具体需求，同时也适合您的能力和资源。如果您不同意，您可以随时做出自己的选择，其实这对您来说可能更可行 —— 这取决于什么对您更重要。

如果您感觉理解这点有困难，请参照这些练习所呈现的思考方式：

[image]

返回：[image]S01E01-T2 识别威胁并作出反应

返回：[image]S01E04-T1 清点您最重要的信息资产

返回：[image]S01E05-T3 确认可能遭受的所有威胁

返回：[image]S01E06-T2 找到弱点建设新的防御能力

返回：[image]S01E06-T3 审核防御能力

当涉及到工具本身时，人们总是试图坚持这7个原则。它们必须是：

1. 开源的

1. 具有足够可信度的（经审计的）

1. 成熟的 (足够稳定，有一个活跃的用户社区和反应灵敏的开发者社区)

1. 用户友好

1. 支持多语种（因此您可以找到自己的语言或进行本地化）

1. 支持多平台 (Mac, Windows, Linux, Android)

1. 有可用的文件资料

如果您认为以上原则没有解决两个重要的问题 —— 即 数据和加密 —— 您是对的；这在后面的内容中会提到这点。另外，关于第1点，我们更倾向于使用自由开源软件 (FLOSS) ，请注意，自由开源软件不一定意味着免费。

以上7个原则可以用一句话来概括 —— 对您作为用户来说，信任应该是指导原则。因为软件是由代码组成的，我们要相信这个代码，而不是那些希望我们使用它的人的空口白牙。如果您在一个黑盒子（专有软件）旁边有一个开放盒子（开源软件）可以选择，请永远选择开放的盒子。推荐或信任黑盒子是有风险的，因为您只能相信制造者所有的承诺，您看不到任何事实证据。

除非您就在那家黑盒子公司内部做关键的工作，否则对于我们这些外人来说，我们不可能知道也无法知道它是好代码还是坏代码。事实上，我们对收集了哪些数据、数据的去向等等几乎一无所知。

请注意，这并不意味着默认的开源就都是好的，事实上，它也是一些人写的一些代码，并伴随着一系列的风险。但是，因为它是开放的，所以可以被验证 —— 这一点很重要。开源的另一个重要之处在于，它带有非专有的许可，允许用户独立行动，与他人分享和改变它。这就是自由的。想要更多理解这点的重要性，请参见：

[image]

延伸：https://iyouport.substack.com/p/-apple-?utm_source=publication-search

不幸的是，开源作为软件的描述已经被过度使用了—— 尤其是那些寡头公司开始采用这一概念之后，这使它变得很混乱。您可以看到在中国发生的事（在硅谷也一样）。一些组件可能是开源的（例如，您可以在设备上运行的应用程序），但是，运行在寡头公司的服务器（云）上的软件很可能是专有的。于是这种 “开源” 是假的。当您看

到中国官方媒体在歌颂开源时，您应该保持警惕。

至于其他原则，在危机时期，人们对便捷解决方案的渴求是前所未有的。不仅仅是用户在寻找，投资者、公司、政府等也在寻找。这时候也是可以出现很多创新的时候。但是，与危机期间的其他事情一样，它往往是混乱的。专注于解决短期问题的需求会引发引入新问题的解决方案。几乎没有时间去测试、调试，甚至理解正在发生的事。这就是为什么对我们来说，在选择想要使用的工具时，成熟度是很重要的。这可能听起来很保守—— 也许是—— 但这也是负责任的、理性的，因为当我们过快地做出决定时，就会有真实的、更长远的后果，这些后果往往是那些最需要保护和照顾的人所经历的。

第3部分：一些基本工具的建议

[image]

本站S01～04中有很多基础安全工具推荐，这些工具都符合上述原则，工具-Tools 专题中收纳的是新生工具。希望您已经在使用其中一些必要的工具。希望您运行的操作系统是更新版本，您的所有应用也都更新了……。

[image]

返回：[image]一句话安全须知：记住这些句子，以简单地优化您的安全性

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法S03E06

返回：[image]S02 在敌对环境中保护自己 - 总章节：低技术含量小洁癖护身法

从设备上管理您的在线通信

对网络浏览器的建议：

TOR BROWSER

FIREFOX

CHROMIUM

BRAVE

推荐的附加组件

—— 选择正确的搜索引擎作为默认搜索引擎，并安装一些附加组件，至少包括：

HTTPS EVERYWHERE

UBLOCK ORIGIN

(可选) FACEBOOK CONTAINER

电子邮件：

THUNDERBIRD

密码管理器：

KEEPASSXC

即时通讯工具：

SIGNAL

安全文件存储：

VERACRYPT

CRYPTOMATOR

此外选择VPN的技巧：

[image]

返回：[image]如何检查您的VPN连接是否实际加密

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

并不是每片云都有一线生机

请记住，“云” 实际上是别人的电脑。有大型（黑盒子）集中化云 —— 要么是供您运行服务的服务器（如亚马逊、微软），要么是存储和处理您的数据的平台（如 Facebook、Alphabet 或其子公司，如 Instagram、谷歌地图、Zoom、Slack等数百个）。

[image]

延伸：https://steemit.com/internet/@iyouport/7jsklp

还有中等规模的云。这些都是由相对较小的运营商运营的，他们可能有自己的基础设施，为您提供专门的服务（开放盒子，例如

Greenhost），也可能为您提供您需要的东西；但是，他们也依赖于上述集中化的大型云。

最后，还有一些小的云 —— 由机构、组织或个人自己运营的自托管的云服务（大多是可以自己控制的）。是的，您可以自己控制，需要一些基础知识，https://iyouport.substack.com/p/nextcloud-?utm_source=publication-search

[image]

并非所有的云都是平等的。您应该选择那些尊重用户及其权利和自由的中小型云，以及那些依靠开源解决方案和不以个人数据货币化为基础的商业模式的云。

"云" 作为一个概念是非常重要的—— 它允许多个客户（笔记本电脑、手机）做更多的事。您的浏览器或手机上的应用程序，成为一个更强大的系统的接口，从远程位置为您提供工具和内容—— 假设您有足够的权限，有便宜和快速的互联网。其优势在于，您的数据更具移动性，您可以从不同的设备和地点访问数据，并且您可以轻松地与他人分享数据。

这些不是唯一可用的模式。许多依靠云计算的活动，例如文件共享，也可以由您的设备来处理，您可以直接与对方做许多事，就是所谓的点对点或P2P模式。Bit Torrent 这种文件共享技术就是一个例子。许多电脑游戏公司使用P2P来发布他们的游戏。

其他的例子还有匿名工具Tor和加密货币，这可能是目前最著名的基于点对点的网络。

用户需要的系统是去中心化的、分布式的、允许互操作性和点对点通信，并且不需要沉重而昂贵的中央基础设施。

事实上，现在每个拥有笔记本电脑或智能手机的人都在以某种方式依赖云服务。有些人几乎所有的事务都在（大型）云端完成。提供云计算和服务几乎是所有监视资本主义公司的巨大收入来源，包括 Alphabet、苹果、亚马逊、Facebook、微软和 Netflix 等寡头公司。

但像 Ube r和 Zoom 这样的公司也遵循同样的模式。他们运行基础设施，他们收集所有可能的数据。

您得到的是通往该集中式基础设施的接口，并享受高效工具的好处；但是，您失去的是所有进入那个积累和聚合系统的私密数据。您同时放弃的 —— 也许对社会更重要的 —— 是聚合的知识。

正如我们在 S03系列中强调的，极简主义是一种安全智慧。在使用和选择云服务时，请寻找尽可能收集最少数据、分享最少必要数据、存储最少必要数据的服务和工具。如果您必须为他人提供服务，比如组织活动、保存邮件列表或进行调查，如果您不需要收集哪些数据，就不要收集。如果是您必需收集的数据，要做到透明化，尽可能减少数据，并及时删除您不再需要的一切数据。

如果您别无选择，不得不依赖 Facebook 和其他流行的平台，需要一些简单的步骤帮助您更好地控制数字隐私、安全和福祉。比如：

[image]

返回：[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗

返回：[image]社交媒体上的行动主义安全性:框架手册

返回：[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

返回：[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

返回：[image]技术增值部分-最简单的分身方法：完美隐身 S04E04

对我们来说，帮助用户意识到他们的设备屏幕背后发生的事，无论他们使用的是什么平台，都是做出明智选择和了解技术背后的政治及其

对生活的影响的一个很小但非常重要的步骤。

[image]

加密的重要性

虽然可以根据上述原则推荐在线或云端工具，但也必须对它们进行评估，以保证通信的保密性和安全性，例如端到端加密。

什么是端到端加密？它是一种技术，它可以让您向另一个人发送一些东西，只有您和对方可以阅读它。其他人可能会看到这种通信，但他们（通常是服务提供商）可以看到元数据，这意味着他们仍然可以看到您正在发送消息、从哪里发送、何时发送、多久发送一次，以及发送给谁。他们只是不能看到您所说的内容。

[image]

返回：[image]泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

很多不同的服务都使用加密技术。它使您能够安全、保密地在网上做一些简单的事，比如网上银行或购物。请注意，有些通信服务承诺用户“可以进行端到端加密”，但实际上他们只对您和他们的服务器之间的内容进行加密，然后再对他们和您通话的对象进行加密。这样一来，当您说话的时候是安全的，但服务提供商可以访问所有未加密的信息。从这个意义上说，您的信息只有在移动时才会被加密，但如果您的信息被服务提供商访问、处理、分析或重新使用，那么在技术上就得不到保护。

端到端加密还有一些其他限制。有时公司声称他们正在使用端对端，但普通用户很难验证这一点。有些服务是选择性加入的，而有些服务只是部分加入。例如，加密可能只对一定规模的使用有效，例如只在两个参与者之间使用，但是对群组聊天无效（就像 telegram 那样）。或者，当您以一种方式使用某项服务时它可能会很好地工作

—— 例如，您的 iPhone —— 但对于其他相关的服务，例如备份，就不起作用。这使得用户在不检查所有细节的情况下，想要导航和做出好的决定就会变得很棘手。

一谈到加密，一些人就会最先想到“犯罪”——“你肯定是想要隐藏什么才会使用加密”，当权者非常擅长激发和利用这些错误逻辑以反对加密并要求后门。反加密之战经年持久，最近一段时间内不断在升级，我们在列表 -1 中有一个同名板块 https://start.me/w/R0LB55，以收集最近出现的相关动态。

当权者的错误就在于，他们总是将隐私和“犯罪”联系起来，拼命操纵叙事，以动员社会认可他们的错误逻辑，https://iyouport.substack.com/p/--dd7?utm_source=publication-search。这些当权者试图将技术能力强加在人性阴暗面上，以声称保护人权的技术“是坏的”。

[image]

在许多情况下，技术既不是好的，也不是坏的：技术是愚蠢的，但绝不是中立的。

这一切都取决于使用它的人的意图是什么。砖头用来盖房子，也可以用来打人，你不能说因为砖头有可能用来打人，于是“它是坏的”、需要被禁用。

否则就成了菜刀实名制的笑话。

总的来说，有些事您需要记住：

- 了解您所使用的工具的商业模式—— 他们是如何通过免费服务盈利的？
- 阅读条款和条件以及隐私政策（是的，我们知道那东西太难读了……但这些公司必须解释该技术是如何工作的）

- 想想哪种云适合您（大、中、小），如果您能负担得起自托管的费用，最好选择自托管

- 寻找使数据最小化的工具

- 仔细检查您正在使用的加密方式（端到端/传输）

您不需要读懂代码，但是，您必须具备 BACK 技术哲学和技术直觉-Intuition&PhilosophyofTech

在线工具的建议

将上述原则转化为一些建议。

交流和聊天 ——

对于语音呼叫和消息传递：

- SIGNAL

- WIRE

使用时一定要遵守一些规则：

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

【注：Signal和Wire都可以自托管，但这并不简单，因为必须创建不同客户端应用程序的专用版本】

- RIOT

(最简单的 Matrix 使用方式，在这里您必须启用每个聊天室的加密功能。您也可以自行托管)

除了Riot之外，还建议大家关注 MATTERMOST，它有托管选项。

语音和视频群组通信 ——

对于语音和视频群组对话，建议使用：

Jitsi Meet –您可以从其服务器中使用它；也可以获取软件并在自己的服务器上运行。

Jitsi 不是单一服务，而是可以由任何人在任何地方运行的工具，因此与 Skype 或 Zoom 等工具不同，它可以使用许多实例。您可以使用的一些 Jitsi 主机包括：

- GREENHOST
- COLLECTIVE TOOLS
- DISROOT
- 您可以查看这里的列表。

值得注意的是，**Jitsi Meet** 只对两人之间的通话提供端到端的加密服务（这也是这种多人浏览器中视频和音频会议的局限性）。您可以和更多的人一起使用，但您必须信任主机。这并不是 Jitsi Meet 所独有

的：对于大多数可用的工具来说，多用户视频通话的端到端加密仅限于极少数参与者；这可以通过使用传输加密和信任中间的服务器来缓解。

根据经验，Jitsi Meet 在小团体中表现不错—— 最多八到十个人——然后事情就会变得有点不顺利。它还需要参与设备的大量资源——要么拉伸其容量，要么耗尽电池。

如果您需要一个类似于教室设置的环境，有白板，许多房间，聊天，语音和视频功能，以及屏幕，演示和外部视频共享—— 可以试试 BIGBLUEBUTTON。适用于团队会议和网络研讨会—— 因为它也允许外部参与者。它可以处理更多的参与者，对于用户来说，它是一个完全基于浏览器的体验。

如果您认为 Zoom 可以做到端到端加密，那您就错了—— 他们提供传输加密，这意味着您在 **Zoom** 上做的所有事都可能在该公司的服务器上被轻易地解密。 https://iyouport.substack.com/p/-zoomgoogle-meetmicrosoft-teams-webex

我们理解，您可能需要同时和多个人说话，特别是当您试图举办在线会议或培训课程时，但目前 Zoom 有太多的问题需要解决，我们都还在寻找可行的替代品。至少，要考虑使用不同的服务，或者，如果可以的话，把您的工作分成不同的部分。

这是其中一个替代方案：whereby.com。

考虑这些问题：您能不能直播其中的某些部分？能不能开一个网络研讨会，并预先录制一些内容？您能否将您工作中的一些互动部分的规模改为多个较小的小组，或使用多个渠道（例如，一个渠道用于协作文件，另一个渠道仅用于音频聊天，如 MUMBLE）？虽然没有完美的工具，但可能要更有创意地设计规模化的虚拟协作。

[image]

协作 ——

对于共享日历、编辑文档和共享文件的协作工具推荐。

协作套件：

- NEXTCLOUD

和 Jitsi 一样，您可以从 Nextcloud 的服务器上试用它。

共享文件：

- RISEUP SHARE
- ONIONSHARE

如果您正在寻找 WeTransfer 或 Hightail 的替代产品，可以尝试 TRESORIT SEND —— 但请记住，它不是开源的。

共享日历：

- TUTANOTA —— 安全邮件服务，还提供加密的日历

共同处理文件：

- RISEUP PADS
- CRYPTPAD（也可以自托管）

项目管理：

如果您正在寻找一种独立的方式来管理项目，并且您愿意在基础设施

和技能上投资，那么我们会推荐自托管的 GITLAB，它适用于那些具有不同技术水平的人。

这很适合大型团队，多个项目，比如您需要多个任务，任务列表，评论，问题或基本的文本编辑。如果您可以自我托管，并且您不介意学习一下如何使用一个专门为管理代码而创建的工具，那就太好了。或者再次尝试 Nextcloud 带有如 “deck” 等插件。

当考虑到您的网络以及您可能需要或用于通信和协作的东西时，请观看 JULIAN OLIVIER’s LECTURE FROM 2019，他解释了为英国的环保运动 “灭绝叛乱” 建立的一个强大而可靠的协作环境的过程，称为 “全球反叛的服务器基础设施”。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

第4部分：缩小范围，进行长期思考

[image]

当您在促进合作并建议他人使用某些工具时，必须考虑以下这些因素。

- 首先，在互联网上，不是每个人都是平等的。与您交流的人可能对互联网的访问非常有限，或者它可能非常昂贵，或者对数据传输量有限制（视频传输会吃掉很多数据）。

- 第二，他们也可能使用过时的或不安全的设备，或者他们可能与他人共享设备。

- 第三，他们的技术、社会、经济和政治环境可能更不可靠、不安全和不可预测。他们与您沟通的事实可能会暴露他们的弱点、地位、观点、信仰或团体，这可能会使他们面临严重的风险。

仅仅因为您能做一些事，并不意味着其他人也应该跟随您。当您邀请他人参与您的流程时，请仔细考虑您为他人做出的选择。

只要您在网上，您就很可能会被追踪

甚至在您打开您最喜欢的应用程序之前，您就已经被跟踪了。这就是智能手机的工作方式，以便为您提供“服务”。

工作原理是，手机不断地被移动服务供应商精确定位，以确保最好的信号，这样用户就可以在移动时拨打电话和获取数据。但是，这些信息足以相当精确地确定您的行踪、揭示您的身份，这些数据可以转化为非常敏感的行为数据 —— 比如您住在哪里，如何通勤，与谁互动，对什么感兴趣。

您可以从下面这些内容中了解一部分具体的危险：

[image]

返回：📱警察如何利用抗议者的手机追踪每个人

返回：[image]你的手机如何背叛了民主？

返回：https://iyouport.substack.com/p/-snowden?utm_source=publication-search

返回：https://iyouport.substack.com/p/b0e?utm_source=publication-search

返回：https://iyouport.substack.com/p/60e?utm_source=publication-search

返回：[image]手机应该有且只有一个用途：如何在敌对环境中保护

自己 S02E03

现在在全世界很多地方，电信公司正在使用并与政府和公共机构分享移动数据，以跟踪、监测和隔离冠状病毒的传播，同时也是为了了解有多少人呆在家里，并确保他们呆在家里。全球各地每天都有关于这方面的新闻报道出现。在其他地方，政府正在与情报公司合作以监视所有公民，比如英国的 Palantir 公司。或者他们使用的工具生产的 SUCH COMPANIES AS NSO，为了支持大规模的情报收集和入侵公民。您可以在我们的 https://start.me/w/74wjJY 栏目中看到非常多的相关揭露。

剑桥分析公司的丑闻暴露了定向广告和心理操纵的使用—— 这两种方法已经被采用很多年，但只有那些从中赚钱的人知道。利用大数据（地理定位）追踪和遏制冠状病毒的传播，将有望再次暴露一些一直存在的问题 —— 就如斯诺登不断强调的：智能手机本身就是追踪器。如果您的手机启用了GPS，这些数据会变得更加丰富和精确。

在共享大数据的背景下，我们经常听到另一个神奇的词："匿名化"。指的是一个将数据与用户身份分离的过程。这意味着，你可能能看到我的数据，比如我喜欢吃什么，或者我多久打一次车，但你不知道我是谁。但不幸的是，匿名化与 "安全" 都是一种愿望，并不是可以实现的永久状态。安全性是一个需要维持的持续过程；匿名化是一个给用户和收集他们数据的公司一些保护的过程。

然而，如果您有足够的耐心和手头足够多的数据集，这个过程往往很容易被撤销。有很多例子表明，数据集去匿名化并重新识别为个人并不难做到，往往会暴露出用户最致命的信息。

[image]

返回：[image]即使数据是匿名的，您的身份仍然可以被识别

您可以看一个简短的片子：

https://vimeo.com/195500135?fl=pl&fe=sh

集体问题需要集体行动

民间社会没有强大的、尊重隐私的工具，因为几乎没有人投资于这种工具 —— 既没有投资者，也没有政府或私人资助者。矛盾的是，这些人往往是第一个要求推荐安全工具的人，并抱怨所推荐的工具不能真正满足他们的期望。

技术对于个人、组织、整个公民社会和公共领域都是至关重要的。人们不得不单单依靠私营部门，要知道私营部门的主要决策工具是利润，这本身就是个悲剧。目前，主流的工具和平台大多都是在美国的，一少部分来自中国（如 TikTok等）；其余极少部分来自俄罗斯（如 Yandex）等国家。所有这些解决方案大多基于对个人数据的利用。

您可以在这里看到下面这个全球概览：

[image]

技术需要钱 —— 很多钱 —— 不仅要创造工具，更重要的是要维护它们。它们运作所需的基础设施更是昂贵。而更关键的是，创建和管理这些工具的人所需要的技能，总之没有便宜的东西。如果我们希望组织能够依靠持久可靠的解决方案，他们就需要获得专门的知识和资源，以自我托管他们所需的服务，或者拥有大规模工作的替代选择。目前，这两方面都不到位。

仅仅不使用 Facebook、避免使用谷歌、甚至在手机上安装定制ROM（操作系统），或者完全依赖开源，已经不够了（虽然我们仍然在这么做）。说实话，现在需要的是集体行动 —— 并不是试图回到数据成为十亿美元资产之前的旧时代，而是向前走。

[image]

这是一个重要的时刻，我们要了解我们所拥有的选择有什么问题，以及这些做法对不同部门（如教育）、对需要它们的社区和整个社会有什么影响。

这是一个极好的时机，可以重新评估我们所需要的工具以及我们需要这些工具的原因，并对创造符合公众利益的可行替代方案进行创新。

抗击冠状病毒需要合作、团结和联网。它需要良好的科学和出色的决策。所有这些应对措施都需要得到技术的支持，或者被技术所利用。现在是决定您站在哪一边的时候了。

这篇文字的大部分内容都集中在个人和小团体的需求和技术上，他们可以在远程工作高度化的时代使用这些技术。值得一提的是，当涉及到更大的机构和组织时，本文中所概述的问题就更大了：基金会、大学、学校、医院、援助机构、正式和非正式网络。所有这些较大的实体也不得不在一夜之间转向虚拟的运作模式。他们现在正在对平台、供应商、服务、工具和应用程序做出关键性的决定，却没有适当的时间来培训如何使用这些技术，而且往往没有额外的资金。

他们必须审视自己拥有的资源、义务、期望和需求。同样，效率也很重要，往往比其他事情更重要。就机构而言—— 就个人而言也一样—— 很难想象一个世界，例如微软、谷歌和 Zoom 没有为学校提供便利。这些服务无疑让学校变得更高效、更便宜、更容易实现虚拟，但是，它们带来的问题与我们一直在讨论的大型平台和权衡的问题相同。

[image]

想象替代技术需要想象替代性的技术政治（比如谁收集数据，如何收集，谁从中受益），尤其是替代性的商业模式，

打破监视资本主义体制 —— 如果将税收贡献用于创造公益技术，会发生什么？

我们不是在做远程工作或远程教育，好像一切都很好；我们正在努力工作、学习，在巨大的健康危机中继续做重要的事。没有人知道这种情况会持续多久，但我们知道它将扩展到我们生活的方方面面，它将改变我们未来做事的方式 —— 国内、职业、社会、经济、政治等等。机构、组织、政府和个人现在做出的决定将决定我们未来的工作方式。

请记住，目前为止都完全没有以硅谷思维开发的工具适合这种目的。不要让冠状病毒的即时性蒙蔽了双眼，不要把自己锁定在不适合公民社会需求的技术中，从而看不到长期的后果。

我们也要利用这个时间来反思和重新思考。这种突然的放缓、封锁和彼此分离很可能会在不同的地方持续很长时间。没有人知道它会变得多么糟糕。在某些情况下，它将使专制政权和寡头联盟能够攫取更多的权力。

然而，这也可能是一个清晰、认识、团结和协作的时刻，所以，当我们从这个时刻走出来时，会有很多事情要做。也许现在我们有了一个很好的理由，花点时间、投入资金并找到支持去做正确的事。

[image]

技术是愚蠢的，您的智能手机是愚蠢的，人工智能也是愚蠢的。问题是：我们这些人类能有多聪明……

[image]
❤🔥

行动安全性-OPSEC

放下功利心名利欲的那一刻，您就提升了至少一半的安全性。这绝非笑谈。 在下一波激烈的街头浪潮来临之前 —— 学习如何制作和使用盾牌、加固横幅，如何保护自己和队友免受橡皮子弹、水枪、警棍、胡椒喷雾、监视和大规模抓捕的攻击。 防御能力是所有行动的持续性基建。 日常练习。熟能生巧。让您和队友习惯于安防措施和机动性的完美契合，你们就可以快速抓住任何机会窗口。

[image]

行动安全性总述

[image] 关键词	个人 团体 行动 防御
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛 ；⛑自卫措施
[image] 创建时间	2018年1月1日
[image] **Description**	行动安全性

行动安全（OpSec）和安全文化有着相近的含义，但是各有侧重，它们都是激进社区抵御镇压的安全实践中不可或缺的组成部分。

做好准备。

1、不要孤军奋战。

尽可能有个伴儿。这是重要的安全问题。

请务必选择值得信赖的朋友结伴而行 —— 最好是曾与你共同参与过激进行动/活动的人。这种团体被称为“亲密团队”。

事先商定行动目标，及各自需求。

- 🔙 [image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

2、掌握基本安全准则。

敏感信息应遵循"按需知情"原则共享：如果某人无需知晓某事项，就绝不应透露任何相关信息。不论此人与您多么亲密。

切勿谈论自身或他人参与高风险活动的事宜，避免炫耀、八卦，更不要妄加揣测。

了解并遵守每位互动对象的安全期望，尊重个体差异。

未经明确同意，绝不泄露可能危及他人的任何信息。

- BACK [image]信息最小化原则

3、了解基本数字安全知识。

只要条件允许，请将手机留在家中。不论聚会还是行动，都是如此。

如果必须携带手机，请提前备份数据，并彻底删除所有您不想被条子拿走的信息。

设置复杂的长密码。

仅通过加密通讯软件收发消息。

如果需要使用一次性手机，请确保所有联系人都熟悉并熟练操作原则。

- BACK [image]安全是追求，而不是任务：整体安全S01E08 - 准备好进入行动

- BACK [image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

- BACK [image]匿名手机

4、着装需保护隐私。

如果可能接触高风险活动区域，请携带能完全隐藏身份且符合人群特征的替换衣物。

更换衣物时避开监控摄像头。

注意包包、鞋子和配饰等细节是否可能暴露身份。

- BACK [image]匿名着装

5、很大程度上激进行动都无法预知事态发展，因此，做充分准备没有错。

请携带耳塞，如果存在任何抛射物的风险，务必佩戴头盔。

确保您的所有队友都熟知战术配件的挑选方法和使用方法。

- BACK [image]头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

6、如果存在化学武器被使用的可能性，请考虑携带防毒面具和/或护目镜。

本栏目收纳的指南详解了警察及其他雇佣军用于恐吓民众的各类弹药，并指导如何保护社区免受其害。针对化学制剂与弹丸对眼睛和肺部的威胁，您拥有多种防护选择。

本栏目已详细列出各类装备的优缺点，助您挑选最适合的装备。

- [image]抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

7、街头购物时请使用现金。

信用卡消费记录和银行账户的ATM取现地点都可能被用于追踪你的行踪。

此原则同样适用于在线转账。

注意元数据问题。抗议活动结束后，切勿在未删除元数据的情况下发布照片。

你可以通过截图快速实现这一操作。

- [image]匿名购买
- [image]在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作

8、为最坏情况制定预案是必要的。

务必掌握最近设有创伤中心的医院位置、前往路线，以及示威活动中若有人遭受枪伤时的应对措施。

- [image]如何处理枪伤：街头实战指南 S05E04

- [image]如何在大规模枪击案中幸存：反侦基础课 S06E09

9、了解警方战术，例如围困战术，并思考一旦遭遇逮捕，应如何应对。

接受讯问时，行使保持沉默的权利，并强调希望与律师交谈。

在任何情况下都不要向拘捕者透露其他信息。

- [image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

- [image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

10、学习如何应对重罪审判，以防万一。

- [image]如何在重罪审判中以及狱中，保持清醒：审讯心理学 S07E04

11、最后，不要只是旁观者。设定目标并实现它们。

关注直接行动全流程指南。不论您和亲密伙伴准备进行到哪个层次、或者预期如何，请确保大家都熟悉并能熟练掌握全部步骤方法和详细资源。保持敏锐，灵活机动。

- [image]直接行动分步指南：它是什么、它有什么用、如何获得成功

[image]

向所有站出来抗争压迫的人们致以诚挚谢意！ —— 无论是走上街头、在后勤工作中努力、从各方面提供各种支援，还是以其他方式参与进来。

我们享有的所有自由，皆源于那些曾经挺身反抗暴政的先驱者。

[image]

[image]
[image]

直接行动分步指南：它是什么、它有什么用、如何获得成功

[image] 关键词	亲密团队 会议 准备工作 协作 反叛 威胁模型 战略图谱 无政府主义 直接行动 组织 行动 街头
[image] 关联	行动安全性总述
[image] 创建时间	2025年1月2日
[image] **Description**	行动安全性

简单地说，直接行动意味着省去中间人：自己解决问题，而不是向当局请愿或依赖外部机构。

任何避开法规和代表、直接实现目标的行动都是直接行动 —— 它包括一切，从封锁机场到帮助难民逃到安全地带，以及组织计划，将你的社区从对资本主义的依赖中解放出来；开发自由软件帮助人们摆脱监视资本家的控制，组办社区家庭教学，帮助孩子摆脱义务教育的洗脑 …… 以及更多方式，所有这一切都是直接行动。

- Table of Contents

  概括直接行动：循序渐进指南
  1、首先**...** 头脑风暴：选择项目并制定计划
  2、确立目标 **——** 确立行动目标并确定其优先次序
  结构
  1、亲密团队**——** 与您熟悉和信任的人紧密合作

2、招募—— 慎重 引进其他个人和团体
3、权力动态—— 确保权力在您的团队中均匀分配
基本准备
1、安全文化 —— 以 [image] 信息最小化原则 的标准传播信息
2、法律支持—— 准备在行动期间和之后提供支持的基础设施
3、媒体 —— 确立您想要的影响力覆盖面，并获取之
基础工作
1、规划—— 研究背景，制定战略，为不同的情况制定计划
2、准备工作—— 准备好装备和适当的服装
3、侦察—— 研究行动现场，掌握变化情况
4、角色—— 划分责任，建立决策结构
一些潜在的角色包括：
5、考虑行动对他人的影响方式
行动期间和之后
1、意识—— 在整个行动中保持警惕
2、沟通—— 互相通报情况
3、分散—— 撤退
4、汇报—— 重新聚集在一起，讨论什么是成功的，什么是可以吸取的教训
最后

[image]

本文将介绍组织和开展直接行动的步骤指南，从最初的计划阶段到最后的汇报，包括法律支持、媒体策略和适当的安全。

[image]

返回：

有无数种情况都可能让人们想要采取直接行动。也许卑鄙的跨国监视技术公司的代表正在你的城市举行会议，他们的监视技术卖给暴政用来抓捕和判罪异议人士，而您想做的不仅仅是站在门外举个牌子；也许这些资本家已经占据你的城市很久，土壤被污染、牲畜死亡、人类患病，而这些工厂继续剥削工人并不受惩罚，您想阻止他们的恶行；也许您想组织一个节日性的、面向社区的活动，如街头派对，以凝聚反抗精神 ；也许看到人们不打断被社交媒体情报抓捕，希望为言论自由开辟一片空间……

直接行动可以包括在废弃的土地上种植一个游击花园，或者用破坏推土机的方式来保卫家园；可以占领空旷的建筑来安置无家可归者；开发安全去中心化自由软件替代品分发给人们 ……

无论您是与几个值得信赖的亲密朋友秘密行动，还是与数千人一起行动，基本要素都是一样的。

概括直接行动：循序渐进指南

1、首先... 头脑风暴：选择项目并制定计划

头脑风暴可以从您想要解决的问题开始，或者从您想要做出的社会贡献开始；它可以来自您所拥有的资源、您所渴望的经验、或您想要合作的人提供的信息。

您可以策划一次短期的冒险，也可以策划一次长期的活动。

通常情况下，最好的头脑风暴发生在非正式谈话的过程中—— 相信您最疯狂的想法可以变成现实，并希望尝试一下。

同样的道理，即使是参加别人组织的活动，最好也要自己带一个计划，这样您才能以自己的方式做出贡献。

[image]

如果您的行动有意义，可以公开组织，建立一种形式，比如公开集会，在其中制定战略和战术。邀请朋友，或散发传单，或挨家挨户地宣布。

提前想好自己的方案，以防别人没有方案。

如果想采取更秘密的行动，可以和一两个值得信赖的朋友在安全的环境中进行头脑风暴。在你们商量好的时候，把你们的想法留给自己，这样当你们准备尝试的时候，它依旧是最新的。

2、确立目标 —— 确立行动目标并确定其优先次序

您的行动是为了谁？是针对现场受众、企业媒体观众、特定企业的老板、股东、警察和政府、其他社区成员、还是参与者本身？

它要达到什么目的？是为了沟通思想、呼吁人们关注不公、激励人们、确保资源、设定特定的基调、造成显著的物质损失、提供一种威慑、展示一种他人可以应用的反抗模式 …… 还是作为参与者的学习和联系经验？

从一开始就建立对行动目标的共同理解，可省去以后当您的计划改变和潜在冲突出现时的很多麻烦。

[image]

结构

1、亲密团队—— 与您熟悉和信任的人紧密合作

直接行动组织的最有效和最安全的模式之一就是亲密团队模式。

[image]

返回：[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

亲密团队是一群彼此间能够深深信任、有着相同目标的朋友，经过长期合作，彼此了解大家的特长和特点，整体会变得高效、行动更有效。

对于一个小的行动，亲密团队的成员可以承担不同的角色。对于一个较大的行动，您的亲密团队可以与其他亲密团队以 “集群” 的形式进行合作，每个小组扮演一个角色。这可以使决策比在一个大的群体中更容易，因为每个群体都可以派一名代表参加发言人会议。

[image]

在这个页面看到单独团队和运行“发言人委员会”的安全措施：[image]信息最小化原则

亲密团队的集群可以长期合作，建立信任和效力。

2、招募—— 慎重 引进其他个人和团体

一旦您有了一个计划建议，就想好您需要多少人去完成它。

如果您的计划需要保密，就只邀请您信任的人加入，而且您还应该确信他们会愿意加入—— 您邀请的每一个人如果最终没有参加，那就是一个不必要的漏洞。

[image]

逐个发出邀请，不要群发邮件！这样那些决定不参加的人就不会知道其他参与者的任何情况。

先问一些关于潜在参与者可能感兴趣的一般性问题，在他或她准备好做出承诺之前，不要透露计划的任何关键细节，如确切的目标或日期等。

当人们被带入计划并继续引入其他人时，要确保每个人对适当的安全程度有相同的理解。

随着越来越多的人参与到行动主义项目中来，重要的是每个人都要明白对他们的承诺有多大的期望。

有时，最先提出计划的团队会比其他人更投入；如果他们做了几个月的准备工作，却在最后一刻导致另一个他们所依赖的团队退出了，那么所有的工作都白费了。

每个人都有共同的责任，从一开始就要坦诚地告诉大家，对他们的期望是现实的。同时，那些发起项目的人应该非常小心地与其他所有参与者分享所有权。信任分级。

3、权力动态—— 确保权力在您的团队中均匀分配

以参与性和协商一致的方式作出所有决定。如果您的小组规模足够大，可以使用非正式或正式的协商会议程序，以确保所有的声音都能被听到：共同制定每次会议的议程，并挑选一名主持人，以保证事情正常进行。

[image]

每个人的参与度越高，您所做的决定就越有依据。

要注意可能不平衡的内部权力动态，例如不同背景的人之间的动态，或本地组织者和外地参与者之间的动态。

每个人越是深入地参与计划和准备行动，大家就会对行动的成功越是投入。一个具有良好内部动力的小组比任何个人都要聪明；个人可以带来想法，但小组可以一起找出应用这些想法的最佳方式。

确保每个人在整个项目中都能感受到支持和舒适；在正式的结构之外和结构内部都要互相检查。虽然经常被忽视，但保持士气是成功的直接行动组织的一个重要方面。在面对意外和不确定性时，要保持冷静的头脑。

[image]

返回：[image]充分的准备和应急反应同样重要：整体安全S01E07 - 计划是 “活的”

[image]

基本准备

1、安全文化 —— 以 [image] 信息最小化原则 的标准传播信息

安全文化是一种避免不健康的偏执狂的方法，在任何时候都要把风险降到最低。如果您和您的朋友们总是明智地进行自己的行为，您就可以减少对 渗透者 和告密者（线人） 的恐惧。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

安全文化的精髓在于，信息是在 [image] 信息最小化原则 的基础上共享的。在某些情况下，您的行动需要全城的人都知道才算成功；而在另些情况下，关键是永远不要在直接参与者的圈子外谈论这个行动。

每个参与行动的人都需要分享一种意识，即认为什么程度的安全是合适的，并尊重他人的安全需求。

[image]

在安全问题上，“同意” 和性亲密关系一样重要；在安全问题上违反他人的意愿是绝对不能接受的。从一开始就必须明确自己的安全需求；必要时一起宣誓保守秘密。

除非得到当事人的明确许可，否则永远不要谈论您或他人参与过的行动，无论过去的时间有多长。

当一个小组聚集在一起进行一个项目时，要确保在场的每个人都得到小组中其他人的担保—— 担保他们是可靠的和值得信赖的。为了保护所有人，您应该准备好在面对审讯和法律压力下保持沉默。

[image]

返回：

从一个项目开始，您就应该按照它可能要求的最高安全级别来操作；您以后总是可以变得不那么谨慎，但如果您一开始就粗心大意，就等于对自己关闭了很多选择。

[image]

要知道您的所有行为都可能被监控或追踪：监控摄像头的记录、您的购物记录、您去的地方和与您见面的人、会议的地点、您扔进垃圾桶的物品、您访问的网站、您电脑上的文件、您留下的[image]指纹（例如，在手电筒内的电池上），以及几乎所有与手机有关的东西。必要时设计强密码，准备好不在场证明。

[image]

从威胁知识库进入相关主题页面：[image]监视器排查 ；[image]匿名购买 ；[image]监控侦测 ；[image]关系网络图谱 ；[image]数字技术限制和最佳实践 ；[image]手套 ；[image]DNA最小化方案

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法S03E06

2、法律支持—— 准备在行动期间和之后提供支持的基础设施

参与行动的每个人都应该意识到并准备好他们正在承担的风险以及与之相关的潜在刑事指控。

重要的是，不要把事情做得比您觉得准备好的更远：如果您在参与某种程度的风险时受伤或被捕，而您对这种风险还没有做好情绪上的准备，它就只会暴露您的脆弱性。

比起，比起匆忙地参与一项行动、然后一塌糊涂、再然后发誓“再也不玩了”…… 您最好还是尽可能慢慢地开始，稳步地建立一个可持续参与的直接行动项目，最好是希望它可以持续一辈子。

如果您的行动可能会导致逮捕，那您就应该提前为所有参与行动的人准备一个法律支持结构，这是必不可少的。这可以包括为被捕者提供一个法律援助号码，法律观察员监督和记录警察的行动，保释金，为被捕者提供即时支持并在法庭上代表他们的律师，以及一个准备在整个法庭案件中提供情感、财务和后勤支持的合作者圈子。

[image]

法律援助号码应该在整个行动中随时开放，接受来电；请记住，在某些情况下，您无法从监狱里打电话！

法律援助号码 不应导致被捕者或接电话的人被指控 —— 如果您的不在场证明的一部分是您不认识对方（您的队友），那你们就不能都从监狱里拨打同一个号码。

如果您担心自己会忘记这个号码，可以用永久记号笔写在身上的隐蔽部位。操作法律援助号码的人应该知道可能被逮捕的人的真实姓名，以便查询他们的情况。

如果您有被逮捕的危险，请决定您是要带着身份证明以便加快处理速度，还是不带任何身份证明，这样条子就不能立即认出您。

[image]

如果能有一大群拒绝提供信息的被捕者，就会束缚法律程序，有时还会获得讨价还价的权力 。团结就是力量的现实佐证。

如果您需要吃药，可以考虑把药藏在身上，或者随身携带医生的说明，解释您需要什么。

找一个有同情心且值得信赖的律师—— 或者可能找多个律师，因为一个律师不能代表同一个罪名的多个被告。

您可以研究一下哪些律师在过去处理过类似的案件。如果您不透露任何敏感的信息，可以向有同情心的律师询问与假设行为相关的指控，或者指定您可能需要他们服务的日期和时间—— 但不要让他们知道任何可能牵扯到他们的事。

[image]

为了做好他们的工作，律师需要能够证明他们与任何“非法行为”无关。请牢记这点。

任何一个成员可能遭受逮捕的社区，最好提前建立一个保释基金/律师费基金；这可以可以省去很多在紧急情况下的奔波。

举办义演，卖T恤，吸引有钱的同情者募捐，让大学里的朋友帮您预定在他们学校的演讲日期，以换取学生基金 …… 等等；确保资金留在一个公平的、值得信赖的、总是容易联系到的合作者手中。

同样，考虑您的媒体策略是什么—— 将公众的注意力和支持引向被捕者是否明智。

[image]

返回：[image]和媒体说话时如何避免陷阱：街头实战指南 S05E13

3、媒体 —— 确立您想要的影响力覆盖面，并获取之

早在行动之前，当您确立目标并确定优先次序时，就应准确地计算出您希望得到多少媒体报道，从哪些来源得到，以及您将如何获得或避免媒体报道。

这可能意味着撰写并发送一份新闻稿（谁、什么、何时、何地、如何、为什么，都要写清楚）、或公报，在亲密团队中推选一位发言人向媒体发言以代表您的行动主义项目，邀请独立记者参加行动或新闻发布会，传真公告或拨打新闻电话，提供采访（亲自或匿名通过一次性电话），或让您的团体成员自己报道。

如果您想避免某些类型的报道，这也可能意味着指派一名参与者，以确保摄影师不会将相机对准你。

[image]

返回：[image]“不要再拍了！请关闭设备删除影像”

如果您正在与媒体沟通，编写谈话要点、您的发言人重复的声音片段等，以确保他们在媒体报道中得到呈现。

给媒体代表尽可能少的材料，让他们不得不使用您希望他们使用的部分。追踪哪些记者倾向于提供积极的报道，并亲自接近他们，记得斯诺登等吹哨人当年怎么做的吗？

[image]

返回：

如果您有一个网站，把这个网址弄到企业媒体的报道中，利用那媒体的影响力让他们的观众改道到您的媒体上。您也可以自己通过张贴海报、海盗电台、演讲活动或挨家挨户开展对话等方式，向公众提供信息。

如果您的行动需要高度的安全性，请安全地发送您的公报：例如，从一台公共计算机上发送，不留下谁使用它的记录。要知道您使用的设备是如何让您入罪的。相关技巧见：

[image]

返回：[image]与S先生共度美好一天-变得难以被追踪的简单方法 S03E03：反取证技巧

返回 - 威胁知识库主题：[image]数字技术限制和最佳实践

[image]

基础工作

1、规划—— 研究背景，制定战略，为不同的情况制定计划

适当的规划是安全、有效的直接行动的本质。

[image]

牢记您的目标和优先事项、以及您所拥有的资源，规划和比较不同的战略。

权衡每一种战术的风险和潜在的回报：总是选择最安全的方式来完成给定的目标，并确保您能承受得起您选择的风险。

[image]知己知彼，是有效行动策划的第一步：整体安全S01E03- 愿景、战略和参与者

有时会发生这样的情况：随着规划过程的进行，一个项目会变得越来越雄心勃勃，越来越冒险，直到一些参与者开始产生怀疑；这时可能需要制定一个更安全的或缩小版计划，这样它仍然可以进行。

在规划中，有无数的因素需要考虑。您必须根据当前的社会和政治形势选择最有效的战术。您必须选择最佳的行动地点，并考虑到它的所有属性；您必须选择最佳的日期和时间。您必须考虑到其他将在该地区的人，以及他们将如何反应—— 他们是同情您呢、还是可能存在敌对以干扰您的活动？您必须协调行动中不同部分的时间，预测每个部分需要多长时间，并弄清楚参与行动的人将如何沟通。

[image]

返回-相关练习：[image]S01E03-T2 绘制行为者关系图谱

在预测其他人—— 比如说，警察—— 的反应时，要考虑影响他们的因素。

- 如果您有出其不意的优势，那么这种优势会持续多久？
- 会不会有很多人关注这个事件？会不会马上知道您在做什么？
- 周围会不会有中产阶级的市民或记者，他们的存在会不会对当

局的反应造成影响？

- 根据以往警察在这种情况下的行为先例，他们的战术可能是什么？
- 条子的上司是否希望他们对您下狠手？或者他们是否想要避免挑起事端？
- 现场各路条子间的沟通能力如何？行动速度如何？他们具体在哪些位置上？可能会走什么路线？

不要低估简单的后勤事务的挑战，比如在紧张情况下运送人员或通讯。也别忘了规划一个撤离战略。

因为计划很少会完全按照所制定的计划来进行，所以制定出针对不同情况的备用计划很重要。”如果___，我们就___；如果___，我们就___。” 心中要有几个不同的目标，以防您的第一选择变成不可能。有一个基本的沟通和决策结构，将帮助您做好准备，以应对与您想象中的任何情况都不同的情况。

[image]

返回-相关教程：[image]充分的准备和应急反应同样重要：整体安全S01E07 - 计划是 “活的”

小心不要让其他人因您的行动而处于危险之中；当局很可能会指控他们所掌握的任何人犯下最严重的罪行，所以既要让那些冒险的人安全地离开该地区，又要确保不能对其他人提出严重的指控。

在某些情况下，您可以把多层次的小组聚集在一起，每个人都知道大致的目标，但只有少数人知道关键的细节，比如具体步骤是什么、或谁来进行最危险的活动等—— 即 信任分级。

对最好的情况和最坏的情况都要做好准备。新的想法，如果是好的想

法，往往会失败，只因为人们对这些想法的理解不够深入，而旧的想法会失败的原因是大家对这些想法太熟悉了，包括当局！

延伸-相关策略：https://iyouport.substack.com/p/39?utm_source=publication-search

有时，最好的结果来自于在全新的环境中应用熟悉的战术。

回头看看有没有先例，在类似的环境下尝试类似行动的场合。这些可以起到很好的指导作用。

当您积累了多年的经验，并从别人的成功和失败中学习时，您将发展出预测和准备各种情况的技能。

2、准备工作—— 准备好装备和适当的服装

一旦您的计划制定好了，就画出一个时间表，直到您的行动，从大日子开始倒数，确定所有必须到位的环节的最后期限。

在计划的早期，确定您需要哪些资金、材料和其他资源，以及如何获得它们。如果安全是优先考虑的问题，要以一种无法追踪到您的方式获得您所需要的东西。

确保每个人都有适合行动的衣服，包括必要时分层穿不同的衣服 —— 以帮助您在撤离时甩掉尾随者。

[image]

返回-具体相关教程：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

返回-自卫措施相关页面：[image]匿名着装 ；周密的行动计划 ；[image]反监视

考虑到与服装有关的安全问题：如果大家为了匿名而穿黑衣服，要确保任何人的衣服都没有独特的可识别性特征；同样，如果您要随机冒充路人，请记住，您家乡城市的平民服装可能与其他城市不同。如果时间很重要，请确保每个人的手表都是同步的。

[image]

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

仔细检查，确保在截止日期前一切准备就绪。

如果参与者对准备行动的地区不熟悉，要先分发地图。如果需要的话，在行动前在该地区放置必要的材料—— 注意在此过程中不要泄露任何东西！

[image]

对应自卫措施：[image]地形侦查

3、侦察—— 研究行动现场，掌握变化情况

行动前，仔细研究该地区。画出进出的安全路线；寻找藏身之处、障碍物、潜在目标和监视摄像头（包括自动取款机和红绿灯内的摄像头）。

[image]

对应自卫措施：[image]地形侦查；[image]反攻 ；[image]监视器排查 ；[image]藏匿点或安全屋

注意关键距离需要多长时间，并注意关键地点的能见度。条子的老窝离我们有多近，他们需要多长时间到达这里？可不可以制造障碍让他

们延迟？该地区还有哪些人？……

在侦查时，注意不要引起别人的注意，也不要留下明显的经过记录。确保至少在计划行动的同一时间进行部分侦查，如果可能的话，在行动前再次进行快速检查，以确保没有任何变化。行动者的记忆力非常重要！侦查好的信息必须牢记在脑子里，您不可能一边看地图一边行动。

如果您的行动需要完成艰巨的任务，比如爬上陡峭的屋顶，不妨在某个时间点进行实际的练习。

还可以从照片、地图和小册子中收集信息；可能会有航空地图或蓝图。在某些情况下，您可以从旅游中心获得信息，或者打电话，借口提问（例如作为学生想做报告，随便编什么都行），甚至接受导游的指导。一旦您收集了大量的信息，将重要的部分整合成适合您的地图会很有帮助。要注意安全地处理所有文件和文书工作。

[image]

4、角色—— 划分责任，建立决策结构

确定完成您的计划所需的所有角色，并确保每一个角色都得到填补。

一些潜在的角色包括：

- 哨兵—— 发现危险信号时能及时做出反应并安全地通知其他人；
- 侦查军—— 侦查者先行，并对地形做出判断，以制定最合理的下一步计划；
- 媒体发言人—— 确保媒体不会歪曲您的行动，发言人很重要，尤其是确保媒体的报道能覆盖您需要呈现给公众的意义和价值；

- 自己的媒体管理员—— 负责在行动过程中记录真相，包括行动者的做法，也包括警察的行为，并有经验安全地保存和呈现记录；

- 法律援助联系人—— 在有队友被捕的情况下需要联系的人；

- 法律观察员—— 要熟悉法律，尤其是熟悉法律漏洞，以帮助行动者尽可能避免被起诉；

- 医护协作—— 如果有人受伤时，必须联系的人；

- 掩护者—— 负责吸引镇压者的火力，以掩护行动尽可能多地持续，这一角色的队友需要具备足够的逃生技能；

- 自己的旁观者（例如，伪装成路人的队友，可以在必要时进行干预，或者在路障竖立在他们面前时礼貌地鸣喇叭）—— 引导公众、并分散镇压者的注意力，还能调动真正的旁观者的情绪；

- 逃亡时需要的司机—— 驾驶技术必须足够好；

- 运送物资的人 ；

- 接受信息和做出战术决策的负责人 ；

- 进行实际行动的人。

在某些情况下，明智的做法是在重要的角色上安排替补队员，以防在最后一刻发现有人不能参加。如果您事先不知道行动的日期会是什么—— 例如，如果它与您无法事先预测的事件相吻合，如政治犯宣布判决的日期或宣战日—— 则更是如此。

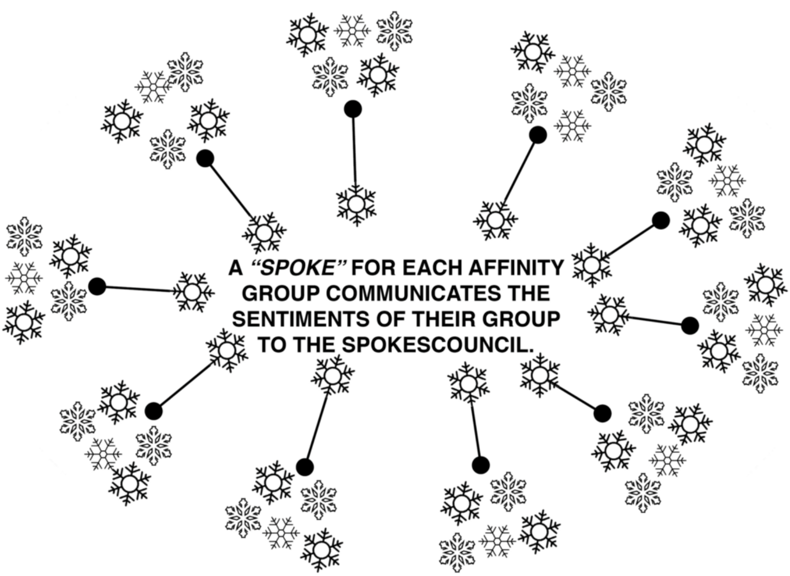
5、考虑行动对他人的影响方式

如果您的行动是在一个较大的活动期间或作为其一部分进行的，那么可能会有一些大型会议，不同的团体会在这些会议上试图协调他们的努力。这些会议可能是有用的，但它们往往会消耗大量的时间和精力，所以确保您在参加会议时清楚地知道您希望达到什么目的。

无论您是在数千名其他活动家中间行动，还是在远离任何人的地方行动，都要考虑到您的行动将如何影响其他人。会不会危及他人？会不会引起警察的镇压？如果会，其他人是否会首当其冲，是否有可能抵消这种影响？您的行动会不会使其他人在某个社区做重要工作时更加困难？在行动前、行动中或行动后，您是否应该进行谈判或做出保证？

[image]

尊重您与其他团体达成的所有协议；有些人可能愿意帮助您，不管是否知道您所做的具体细节。随着时间的推移，如果您证明了自己的可靠和体贴，您就会与他们建立联盟。



行动期间和之后

1、意识—— 在整个行动中保持警惕

意识是任何行动成功的关键。通常情况下，气氛会很快发生变化。重要的是要跟上您周围发生的事，并事先确定您将如何对某一情况作出反应。

例如，一辆警车的到来是大事吗？那十辆呢？在这个城市里，警察尾随游行者是常见的事吗？虽然您永远无法确定到底会发生什么，但提前回顾可能发生的所有情况，并了解您的小组想如何处理这些情况，将使每个人对如何应对—— 以及如何避免过度反应—— 有一个更坚实的想法。

[image]

在向他人通报事态发展时，要公布原始信息，而不是您可能从中得出的结论（是 “警察正在戴上防毒面具”，而不是 “他们要毒死我们！”），这样其他人就可以得出自己的结论。

抵制惊慌失措的冲动，也要抵制得意忘形的倾向。

2、沟通—— 互相通报情况

在行动中，侦察员可以跟踪地形的变化做出反应，如警察的到来、人群的流动、附近其他人的活动和安全区等。他们可以使用通信系统，如一次性电话、加密短信、双向无线电、或哨子，来保持联系；也可以使用音频或视觉信号，如汽车喇叭或烟花。警用扫描仪可以用来监控警方的通讯。

为了提高通信效率，侦察员可以向行动中心的个人或分队报告；在更大的环境中，侦察员可以将自己的发现打电话给一个中央信息枢纽，

其他人可以带着问题直接询问这个中心。

[image]

就像通讯设备可以让您更有效率和效益一样，它也增加了被监视的风险。您可以使用密语和[image]假身份 ，比如12点钟方向有警察部队增援，密语可以是“12点开饭”。

但要慎重—— 使用密语容易被栽赃，检察官可以声称您的密语比实际意义更激烈。

即使没有使用其他通信系统，在紧急情况下选择一个 “中止” 信号也是有用的。比如间谍的常见做法，在一辆车子上挂一个特殊的标记 —— 情报行动前所有参与者都理解这个标记，让其他人都不理解，然后开着车子途径行动者出没的地区，以提醒人们 “行动中止”。

[image]

3、分散—— 撤退

安全逃生是直接行动组织中最常被忽视的部分。一定要事先制定好退出策略。

[image]

返回-相关教程：[image]思考方式是战略性的：完美隐身 S04E03

如果您将在一个大的团体中，特别是和其他没有参与策划过程的人一起工作，想想如何避免从众心理，保持表达自己的权利。

知道什么时候应该按捺住自己的优势，什么时候该退出—— 什么时候该跑得越快越好，什么时候应该不紧不慢地走。

丢弃任何可能使您入罪的东西，如果可能的话，把它放在一个不会被发现的地方；等到您确定甩掉了监视跟踪时，再回来取。

[image]

对应自卫措施：[image]藏匿点或安全屋

如果需要，事后在一个安全的地方集合，确保每个人都有交代；寻求外界援助，写新闻稿。趁着每个人都还在，获取任何可能出庭作证或提供文件以协助被捕者的人的联系信息。

4、汇报—— 重新聚集在一起，讨论什么是成功的，什么是可以吸取的教训

行动结束后，销毁任何可能对您不利的证据；将可能与行动有关的工具放在隐蔽处。

如果您在未来的某一天可能需要出庭作证，请考虑将您可能需要记住的所有细节写在一张纸上，并将其藏在某个您可以确定永远不会被其他人发现的地方。

在一个安全的环境中聚在一起，复述发生的事。跟进正在进行的事，比如支持那些有法庭案件的人，向公众进一步澄清行动背后的目标和想法，以及整理冲突。

庆祝你们的胜利，互相提出建设性的批评，从错误中学习，并为下一个项目制定计划。

最后

本站系统服务于已经有志向、有目标、知道自己要什么的人们。

直接行动不是游戏，不是举牌子那么简单，但它是最可能有效的模式；它要求实践者必须具备足够的知识和技能，以及心理素质和应变

能力， 这需要日常的训练 。

熟能生巧。让您和队友习惯于安防措施和机动性的完美契合，你们就可以快速抓住任何机会窗口。

[image]
[image]

S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训

[image]	关键词	协调 反叛 团体 基准线 态势监测 战术 直接行动 组织 自卫 街头 防御 防暴武器 防身
[image]	关联	[image]直接行动分步指南：它是什么、它有什么用、如何获得成功；行动安全性总述
[image]	创建时间	2025年1月3日
[image]	**Description**	行动安全性

帮您大幅提升战斗力的主要课程。

S05的主题是街头实战。重点关注镇压机构常用的防暴弹药以及抵御方式，以及从整体角度上考虑街头行动的安全性措施。

随着来自警察、间谍、和各种流氓组织的暴力不断加剧，反抗者最重要的是要思考如何保护自己。您需要先活下来才有机会取胜。

没有人应该在保护身体安全和在我们的社区组织之间做出选择——但是，警棍、冲击弹药、和街头袭击，都是为了迫使反抗者在两者之间做出选择。

这不是您是否采用对抗性策略的问题 —— 如今，任何处于抗议情况

下的人都可能成为目标，不管你是不是活动家或者组织者。

通过采取适当的预防措施，您可以减轻风险，同时继续为反抗运动努力。

列表

[image] 认识警棍，危害能力和防御方法：街头实战指南 S05E01

[image] 头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

[image] 抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

[image] 如何处理枪伤：街头实战指南 S05E04

[image] 从雨伞到激光、气球到电动工具：街头实战指南 S05E05 - 战术器具综述

[image] 警用武器常见伤害及基本处理方法：街头实战指南 S05E06

[image] 充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

[image] 了解防弹衣：街头实战指南 S05E08

[image] 您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

[image] 了解防暴弹药，以及如何保护自己 ：示威参与者指南S05E10

[image] 让监视摄像头失明：示威参与者指南S05E11

[image] 在街上保持安全：街头实战指南 S05E12

[image] 和媒体说话时如何避免陷阱：街头实战指南 S05E13

[image] 加固横幅和盾牌的制作和使用方法：示威参与者指南S05E14

🚧 占领街头：封锁和阻断指南 - 街头实战指南 S05E15

[image] 如何启动黑群 - 从准备到行动：街头实战指南 S05E16

[image] 反击, 保持自由：街头实战指南 S05E17

[image]
[image]

认识警棍，危害能力和防御方法：街头实战指南 S05E01

[image] 关键词	街头 警棍 防御 防暴武器
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月4日
[image] **Description**	行动安全性

每一种武器和战术都有其优势，也有其弊端；针对镇压武器和战术，行动者的思路应该是如何尽可能抑制其优势的发挥。

- Table of Contents

  警棍的类型
  1、防爆警棍
  2、可伸缩警棍
  3、侧把手警棍
  常见伤害
  如何防御警棍
  更多相关资源

本集内容将详细介绍警察使用的警棍种类、如何使用、警棍能造成什么样的伤害，以及历史上示威者保护自己免受警棍攻击的一些方法。

[image]

警察经常用警棍打人。从记录现场的录像来看，您会认为这些警察就

是为此暴力而生的。从历史上看，警棍是警察的面包和黄油，以至于警棍经常被称为警官的 “职务徽章” —— 虽然最近，泰瑟枪已经取代警棍成为了他们的首选武器。

那些教学视频和小册子中介绍的“警察”会给人一种错误的印象，误认为警察是武术高手，他们可能早已深入研究了用大棍棍伤人的所有方法。但是，如果您去演示下就能知道，一般只有那同样的几招，一遍又一遍出现。

警察对着已经倒在地上的人疯狂地挥棒，他们用警棍的末端刺向目标人，狂甩上臂挥棒打人，往往是打在头部 —— 虽然理论上，他们不应该这么做，除非他们已经被授权使用致命武力。

有时他们还会将手分别放在棍子的两端，水平地举在胸前，一边向后推人，一边叫着 “滚开”—— 往往不管被推的人是否能动，也不管他们是否已经在动。

[image]

从根本上说，警棍是所谓的合规工具。警棍并不是专门用来杀人或伤人的武器，尽管它们完全有能力做到这点。警棍的目的是为了伤害抗议者，以迫使抗议者服从警官的命令。当然，警察往往在抗议者屈服之后也会继续使用警棍，只是为了强调国家主体和它的权力支柱——即 这些雇佣兵—— 之间的权力关系。

不是每个警察都喜欢警棍。有些警察除非接到部门的命令，否则不会携带警棍。YouTube 上的一位前警察指出，“有效性” 和 “合法性” 在文氏图中的重合度确实非常小。然而，警察很少被要求遵守任何合法性的标准。警棍往往是警察在近距离作战中控制空间的主要手段，尤其是针对示威者。

在抗议活动中，警察使用警棍来完成各种任务。有的警棍被用在冲锋中，大量警察挥舞警棍并推搡人群，以驱散人群和煽动恐惧。这些警员们使用警棍是为随后而来的抓捕部队进入人群实施逮捕，而开辟道路。警员用警棍推进警戒线，推搡抗议者，以便镇压部队可以继续前进，通常同时还用胡椒喷雾袭击抗议者。

延伸：https://iyouport.substack.com/p/--06e?utm_source=publication-search

有些警察是出于纯粹的报复心态或残忍的本性，一旦把人摁倒在地上，就用警棍猛烈地殴打他们。

人们似乎有一种误解，以为警棍只用来对付不遵守警察命令的人。事实上完全不是，警察使用警棍对付他们怀疑可能会阻碍他们实现目标的任何人，无论这个或这些人是否违法或不遵守警察的命令。

警察使用武力的准则一般规定，使用警棍打击目标人的四肢的主要神经中枢属于“中等武力”，而打击目标人的头部、颈部或锁骨，则属于“致命武力”。记录警察暴力的抗议现场的活动家需要记住这些标准，在您拍摄取证的过程中，您需要准确地描述警察行为，以便随后与权利组织合作，让暴行实施者付出代价。

[image] 这是FBI和美国司法部出版的1967年执法培训手册的封面插图。这就是当局希望警察认识自己的职务方式。

警棍的类型

本文将研究3种类型的警棍：定长警棍（或“直棍”，包括防暴警棍）、可折叠警棍、和侧把手警棍。

1、防爆警棍

防暴警棍是一种“直棍”警棍。最常见的例子是36英寸长，直径1.25英寸，由聚碳酸酯或硬木制成，通常是山核桃木，但有时可以是樱桃木、白蜡木或其他木材。

现在一些警察正在采用更粗的棍子，如直径**1.5**英寸的警棍，以施加

更大的打击力量。

警察手里拿着一根1.25英寸的警棍和一根1.5英寸的警棍，其重量和周长造成的攻击力度之差别比您想象得要大。

较粗的棍子本身并不是更好的武器，但它们更结实。如果把两种粗细的棍子放到同一个有经验的打手手中，让他攻击胶合板盾牌，直径1.25英寸的棍子就会折断，但1.5英寸的棍子就毫发无伤。后者施加的力量大大超过了任何一般护盾所能承受的范围。

木制警棍要么是透明涂层的，要么是漆成黑色的。聚碳酸酯警棍是黑色的。防暴警棍有各种不同的握柄，例如在一端或两端刻有环形或凹槽，或交叉的 “压花” 握柄。

这些握柄中的一些设计是为了在警棍被拉动时提供更好的固定性，不至于脱手，而另一些则是为了在扭转动作的情况下提供更好的固定性。

大多数都带有一个简单的皮制套子来固定。一个训练有素的警察应该以这样的方式握住皮带条，即 如果棍子被抓住并被拉到人群中，他可以放手，但许多警察握住警棍的方式是不正确的，在后者的情况下，如果警棍被拉动，无论警察是否愿意，他都会被牵制过来。

聚碳酸酯警棍比木棍能带来更大的冲击力，但价格却大大高于木棍。一些警察抱怨说，聚碳酸酯警棍在夏天会变形，在冬天会碎裂。

防暴警棍是用来打人、刺人和推人的。广义上讲，警察用警棍打击反抗者，并且也用警棍推搡挡在警察面前的游行队伍，这种情况下警察和抗议者会非常接近，用以恐吓抗议者离开一个地区。警棍用于刺伤人也是为了这两个目的。在拥挤的环境中，警察被训练成用警棍的两端同时进攻，以便保持武器不脱手。

警官们考虑在人群环境中如何维护武器的问题相当多。他们的训练重点就是这个。他们害怕有人会抢走警棍，用它来反制警员。

防暴警棍在恐吓方面的作用是很难夸大的。警察在希望自己看起来更可怕的时候，就会挥舞这些大棒张牙舞爪；在某些情况下，他们采用木制的警棍与制服形成鲜明对比，意在激发人们的恐惧。他们在警戒线上时双手拿着棍子，显得不可接近。他们毫无预兆地使用警棍，以使抗议者处于紧张状态。

防暴警棍与传统的固定长度警棍的主要区别在于，后者的长度为26英寸或更短。许多部门在日常使用中采用锥形警棍，这种警棍一端的打击面较宽，另一端的手柄较小，更易控制，形状像狼牙棒。这种警棍为打击提供了更大的杠杆作用。

学会区分这些类型的警棍，可以帮助反抗者弄清警察在考虑采取什么☠镇压手段 ：如果他们挥舞的是较长的防暴警棍，他们预计会使用更多的暴力。

[image]

2、可伸缩警棍

越来越多的警察部门开始使用可伸缩警棍作为日常挂在腰带上的警棍。这些警棍也被称为可折叠警棍或ASP（这本身是个品牌）。

可伸缩警棍的尺寸通常在16″-31″之间，其中16″、21″ 和 26″ 是最常见的长度。它们大多由钢制成，而一些重量较轻的型号则使用铝合金。

握把可以是泡沫胶状的或塑料的，或使用一些其他纹理。闭合后，这种警棍的大小和形状大致相当于一把小光剑，星球大战里那种，挂在皮带上。

警察打开它们的方法是轻抖，用离心力将折叠段滑动到位。大多数这类警棍是通过每个钢片与下一个钢片的摩擦力来打开的，只能通过将尖端砸在水泥地或其他硬表面上来关闭。一些较新型号的这类警棍有一个按钮锁，使它们更容易关闭、和更有效的刺杀以及摆动。警方转

向使用按钮锁式的折叠警棍的另一个原因是，在混凝土上闭合的警棍其顶端很快就会出现粗糙，偶尔会割伤被警棍击中的人。

警察抱怨可伸缩警棍如果整天都用来打人—— 比如在镇压示威活动中—— 就会断裂，而很多大量使用警棍的警察都把警棍当成一次性用品。警用文献中明确提到，打开可伸缩式警棍时涉及到的恐吓因素是该武器的一个优势。

对于对自卫感兴趣的平民来说，可伸缩式警棍是比较常见的。人们在那些处于暴力倾向的情况下，不愿意用带刃的武器或枪支来保护自己的人们更多会使用这种棍子。这种警棍的合法性因地区而异。

3、侧把手警棍

这种警棍是直的，短柄从侧面伸出，距底座约六英寸。

这种警棍是西方从日本的传统武器 tonfa 改编出来的。tonfa（拐）如下图，有多种不同的类型。如二字拐、十字拐、卜字拐、上下拐、鸳鸯拐……等。目前比较常见的是卜字拐为短拐的一种， 是一枝卜字型的棍棒，也有T型棍、旋棍等名称。

[image]

侧柄警棍与这种东西非常像，被认为是一种更具 “防御性” 概念的武器；这种武器被更常用之后，在20世纪60年代从所有的警察暴力镇压民权抗议者的媒体曝光中都能看到这种武器出场。

警察可以通过侧柄握住警棍，因此警棍的长度从前臂一直延伸到肘部。这个姿势用于阻挡抗议者的反击、并通过造成疼痛而使抗议者顺从。警察也可以握住这种警棍的其他部分，于是侧手柄就成为了一种可以阻止抗议者反击的剑柄。

最著名的是，这种警棍由洛杉矶警察局警官携带，并在1991年广受关注的袭击罗德尼·金（Rodney Glen King）事件中被使用。

从那一事件中可以看出，这种所谓的“防御性”警棍事实上是另一种伤害性武器 ，使用方式和警察一直以来使用的任何钝性冲击武器一样，它的所谓“防御性”名声只是一个招牌。

【注：罗德尼·金，非裔美国人，出生于加利福尼亚首府沙加缅度。1991年3月3日，因超速被洛杉矶警方追逐，被截停后拒捕，遭到警方用警棍暴力制服，1992年，法院判决逮捕罗德尼·金的四名白人警察无罪，从而引发了1992年洛杉矶暴动。】

[image] 在抗议罗德尼·金被殴打的抗议活动中，一名警官使用侧柄警棍袭击示威者。

虽然侧柄警棍的设计原本不是为了以侧柄作为击打点的，但很多人都能看到，警察拿着警棍与手柄相对的一端，像锤子一样挥舞。这样一来武器的更多力量被集中在一个点上，可以造成更严重的伤害。

在过去的20年里，侧柄警棍已经不再是警察的日常携带警棍（比如美国警察），取而代之的是可伸缩式警棍。但许多警察都不同意这种转变，有些警察仍然选择携带他们心爱的“PR24”—— 这是一种以标准的莫纳德诺克PR-24式警棍命名的侧柄警棍的通用名称，长24英寸，由聚碳酸酯制成。

[image] 莫纳德诺克PR-24式警棍 [image] 在1992年罗德尼·金（Rodney King）起义后的25年，前洛杉矶警察局的一名警官抚摸着他的侧柄警棍，回想当年警察的暴行是如何导致动乱的。

常见伤害

没有找到很多关于警棍杀伤力的研究，但是，用警棍击打人的头部往往可以致人于死地，这不是什么秘密。我们能够找到的大部分资料都是在英国发表的，这并不奇怪：英国的警察往往不携带枪支，而是用老式的方式伤人、甚至杀人，包括用警棍。

据一位医生介绍，大量的警棍伤是在人举起手臂保护脸部时造成的前臂骨折。不过，对头部的打击，以及胸部遭受的程度较轻的打击，要比对四肢的打击要危险得多，因为这些部位都会造成脑内出血、脑震

荡和骨折。

肋骨骨折在警察从侧面挥击目标躯干的情况下是很常见的。很多人因为试图抵挡警棍的打击而最终导致手臂和手腕骨折。胸部遭受打击的重点是横膈膜，这种伤势可能会造成呼吸困难；再加上惊吓和压力，都会导致人失去知觉或呕吐。

[image]

如何防御警棍

为了避免在近距离战斗范围内受到暴击的伤害，您有三个基本选择：

- 您可以远离近战范围。
- 可以阻止对手清楚地看到您，以便阻止他们有效地打击您。
- 可以直接保护自己和他人免受打击，很可能是通过某种屏障。

警察使用暴力至少有两个目的：控制空间 —— 分散我们这些抗议者，驱赶我们，阻止我们到达目的地 —— 以及制服目标个人。有时，最简单的解决方法就是逃离拿着棍子的警察：通过后退来远离近战范围。

但在其他情况下，这种方法的后果是不值得的。您很可能不希望放弃其他示威者同伴，可能更不想放弃当初把自己带到街上的反抗目标。您可能更不想承认被吓跑掉了。

因此，另一种远离近战范围的方法是迫使警察后退，或者至少让警察不要在抗议者之间拉开距离。

历史上，抗议者经常通过使用自己的投射物—— 瓶子、石头、油漆弹等来实现这一目的。

这可能是有效的，但其效力和可取性是因地而异的—— 这取决于警察的目标是什么、以及限制警察行动能力的其他因素。

您的战术筹备必须符合您的实地因素，以捍卫您和队友的利益。

解决这个问题的另一个办法是修建路障。为了达到目的，路障必须适合于阻挡它们所要解决的特定威胁 —— 想要阻挡警车和阻碍步行的警察，是两个截然不同的目标。

历史上，一些示威者经常通过放火的方式使路障更难通过和难以被拆除；但路障一旦燃烧，除非有无限的燃料供应，否则它最终会自行熄灭。常识性的消防安全措施就可以破灭它；当地法律也很可能禁止这么做。

即使路障完全不妨碍人流，正确的路障设置也可以分散警察的注意力，这也是另一种让警察与抗议者保持距离的方法。只要情况是无法预测的，并且警察必须全方位关注新发展，他们可能会选择不采取那些使自己退缩的方式。

第二种策略是防止警察看清楚你，这样他们就无法准确打击你。抗议者为此采用了盾牌、雨伞、烟雾弹，有时甚至是灭火器等工具。我们曾见过抗议者举着高高的横幅，以至于挡住了另一边警察的视线—— 当然，这些工具也会导致大多数抗议者看不到警察在做什么。

警察讨厌看不到正在发生的事，这可能会让他们后退一步，重新聚集，但也可能激起他们毫无意义地暴力升级。如果警察看不清楚，他们可能就会随意出手—— 对防御来说这未必是一种改善。

最后，如果没有其他办法，还可以直接防备警棍的打击。这通常涉及到装甲、盾牌、移动路障、加固的旗帜、或其他障碍。

为抵御重击而设计的装甲一般采用 “硬壳/软垫” 框架：硬壳可以将打

击的冲击力分散到更大的表面积，而软垫则可以吸收这种冲击力。现在的外壳通常是某种塑料材质，尽管传统上使用的是钢，在某些情况下也可能使用木头；同样，软层通常由泡沫组成，尽管在过去，加垫的衣服也可能起到作用。

如果您正在考虑穿戴任何类型的盔甲，首先要考虑头盔。戴头盔越是正常化，警察就越难以针对想要保护自己的个人（本系列后面的内容将详细讲解头盔）。

头部受伤是很严重的事，反复的脑震荡可能会带来成倍的危险。即使您在经历了头部受伤后感觉一切正常，但头部遭受后续打击的风险也会大大增加。街头的人如果头部受到打击，应该认为自己在之后的一周内都将处于高度危险之中；第一次脑震荡未愈后的第二次脑震荡可能导致死亡。如果您的头部受伤，请考虑至少一周内避免危险。

运动类装甲可以从二手商店轻易买到。大体上，它的设计是为了防止警察警棍可能造成的同样的影响。曲棍球和棍网球的垫子都是可以使用的，它们很轻、低调，并旨在最大限度地提高流动性，同时保护重要区域。

足球护胫板也可以作为前臂护板。被警棍击中从来都不是什么好的体验，是否使用护甲可以意味着骨折与否的区别。

请根据您的威胁模型选择重点保护的部位：

膝盖是致命性较低的弹药的常见目标，

腹股沟是脆弱的部位，

前臂通常用来阻挡警棍的打击，

胸腹部通常容易受到警棍的刺击或冲击弹药的打击。

总之，您越是认为不管发生什么事都需要让自己坚守在第一线，您就越应该考虑什么样的盔甲可以保护自己。

从历史上看，一些运动采用了 “填充物” 的方法来保护人群免受警察暴力的侵害，用泡沫、内胎和其他充气游泳装置，以及其他任何他们能接触到的大型的柔软的东西，来建造不可思议的服装。

这种防御可能严重限制了个人的行动能力，但是，它可能会阻碍警察驱散人群。它还可以创造出引人注目的视觉效果。这种方法最著名的例子是意大利的 Tute Bianche。

从战术上讲，盾牌可以更灵活一些。一个拿着盾牌的人往往也可以保护两边的人。一群拿盾牌的人可以形成盾墙，这比孤盾要有效得多。

[image] Tute Bianche 的抗议队伍 [image] Tute Bianche

移动路障实际上是由多个人携带的多用户盾牌。这些移动路障在人群的前面、侧面或后面特别有用，可以提供掩护，防止警察轻易攻击或驱散抗议者。

一个简单的例子是一块大的胶合板，上面有多个把手，或者后面有一根长柄。在紧要关头，示威者也曾用梯子和其他可自由使用的物品临时搭建移动路障 —— 例如，2010年温哥华反奥运会的抗议活动中使用的那种。

[image] 2010年温哥华反奥运会的抗议活动

也有其他移动路障，比如用透明的钢格板或其他板材装在木架上。有些时候背面装有支架，这样当它们被放下时就可以自己立住。

要制作加固的横幅，可以把乙烯或织物的普通横幅用木头、塑料或其他坚硬的材料做一个支架。加固的作用不仅仅是为了使横幅更容易携带，它们也可以在战术上用于保卫抗议人群的边缘。

PVC管很容易购买，但在受到冲击时比较容易断裂。作为加固横幅的手段，它屡屡失败，最著名的可能是2005年在华盛顿特区举行的反对乔治·布什第二任期就职典礼的抗议活动。

[image] 2005年在华盛顿特区举行的反对乔治·布什第二任期就职典礼的抗议活动

如果您很着急，新鲜的竹竿也可以用—— 它出奇的轻，而且有足够的弹性，对打击有一定的反弹力。

[image]

但是要知道，盔甲、头盔、盾牌、移动路障、加固的横幅、和其他防护装备，都能让您脱颖而出—— 而在示威中脱颖而出很可能并不是什么好事。您应该和您的亲密团队协商这件事，关于这些战术可能的风险和你们的承担能力。

并没有万无一失的抗议方案，也没有完全可以确保有效的战术，没有能解决所有问题或适合所有情况的装备。您需要想一想自己想要完成什么，以及警察可能会如何阻止你完成这一目标。要实事求是— —— 对自己的能力和对镇压者的能力都应该尽可能准确。

移动性、速度、主动性、出其不意的元素，以及持之以恒的反抗意识，通常会比任何装备都更适合使用—— 所以，要确保您的装备不会阻碍或分散您的注意力，使您能最大限度地发挥这些优势。

更多相关资源

[image]

延伸：警棍的技术和使用（PDF）

延伸：FM 3–19.15 —— 警察培训手册（PDF）

延伸：Excited Delirium —— 从2008年开始，由直接行动抗议者制作

的警察武器指南。

延伸：Bodyhammer —— 一份在世纪之交后不久出现的，旨在探索头盔、防弹衣、盾牌和盾墙、以及一系列防御战术和编队的杂志。

[image]
[image]

头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

[image] 关键词	头盔 街头 防御 防暴武器
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年1月5日
[image] **Description**	行动安全性

镇压者都非常明白这点，关于：人的头部是最弱的部位；所以，他们经常将榴弹对准抗议者的头部发射。有效的头盔可以保命，这不是玩笑。

- Table of Contents

  摘要
  一些选择
  为什么要戴头盔？
  挑选头盔
  头盔的种类
  悬挂式头盔
  硬帽
  攀岩头盔
  古代军用头盔
  防撞头盔
  自行车头盔
  滑板头盔和滑雪头盔

摩托车头盔
马术头盔
填充式头盔
1、运动头盔
2、战术头盔
弹道学
风格
侧面防护和护罩
填充物
二手
更多相关资料

[image]

本集将继续前面的内容探讨各种保护性的头盔，详细介绍每种头盔的优缺点，让您可以挑选出最适合自己的头盔。您拯救的生命是您自己的。

[image] 这是抗议者 Aaron Cantu 的头盔，俄勒冈州波特兰市的一名警察故意向他的头部直接发射了一枚闪光弹。如果他当时没有戴上头盔，很可能会被直接炸死。 [image] 2022年底伊朗抗议者的损伤

摘要

如果您没有时间阅读全文，这里是您基本需要知道的：

如果您预计没有其他人会戴头盔，就戴一些隐蔽的或不显眼的东西 —— 比如防撞帽、棒球帽、低调的滑板头盔，或者自行车头盔 —— 这样就不会让自己因脱颖而出而成为被镇压目标。

如果您预计现场有很多人会戴头盔，那就戴上您能买到的最好的头盔，如战术防撞头盔或防弹头盔。

一些选择

高端的—— IIIA级防弹头盔，比如头铁老兵ATE，或者是经过高标准测试的折扣款，如相对比较便宜的 LongFri 款。

更便宜的战术型头盔—— 要么是100–200元的名牌 “防撞头盔”，要么是40元的气枪头盔。如果您选择后者，要把护垫换成真正的护垫，而且不要指望它能提供与高端品差不多的保护。

更便宜的选择—— 找一个最便宜的滑板头盔，很容易找到，这类产品也会宣传自己满足各种认证。

低调的选择—— “防撞帽”（不是 “防撞头盔”）—— 有点像内置在棒球帽里面的硬帽。

在紧急情况下—— 一顶半圆形的或四分之三的摩托车头盔，或者去掉面罩的曲棍球头盔，或者其他任何您能找到的头盔。都比没有的好。

[image] 头铁老兵ATE [image] 防撞帽

为什么要戴头盔？

头是最脆弱的部分。警察非常知道这一点，所以他们瞄准抗议者的头部进行攻击。街头流氓也是这样做的。在很多抗议活动中，戴上头盔是明智之举。

就像所有的装备一样，重要的是要权衡利弊。如果您是唯一一个戴头盔的人，您可能会吸引更多的注意力，那应该不是您想要的效果。如果没有其他人会戴头盔，您可以考虑戴一个不那么显眼的头盔。如果您预计大多数人都会戴头盔，请确保您戴的头盔是质量最好的头盔。

移动性、能见度和灵活性，非常重要—— 无论我们说的是某件装备还是我们的整体行动。

镇压者几乎总是会比抗议者拥有更多的资源；在静态条件下被卷入正面对抗通常是个 错误 。

镇压者的 弱点 是对新信息的反应往往很慢，而且他们普遍缺乏动力和创造力。

所以，在选择装备和战术的时候，抗议者应该始终 以保持流动性和机动性为目标，小心不要因为防御而使自己的负重增加。

去年的抗议活动中，廉价的自行车头盔已经救了很多人的命。如果您不想花钱，那就戴上您现有的任何东西。

溜冰头盔就很好。一顶简单的自行车头盔也比什么都没有的好。全脸的摩托车头盔或越野车头盔价格较贵，尤其是，它们可能限制了您的视力和听力，并带来了其他各种缺点—— 但是，如果您的眉心被催泪瓦斯罐击中，您会非常庆幸戴了头盔。

没有任何一顶头盔可以完全保护您的头部免受打击或射击。没有任何“防脑震荡” 的头盔可供足球运动员使用：这需要大量的泡沫。和所有护具一样，头盔能做的就是减轻某些风险。

人们往往会盯着头盔的外壳—— 比如说，认为既然是可以抵御枪弹的防弹头盔，那么它就会比冰球头盔更能保护头部？但是，防弹头盔只是为了保护您的头部不受枪弹的伤害—— 它可能无法有效地保护您的头部不受冰球的伤害。而曲棍球头盔在交通事故中可能无法像自行车头盔那样保护头部。需要清楚这点。

对于头盔来说，外壳和填充物的比例大致相等。如果弹丸穿透了外壳，填充物就起不到什么作用了。然而，如果外壳本身没有被击穿，那么填充物就能保护头部免受钝性冲击。

弹道学 是一个复杂的领域。长话短说就是：对于一个普通人来

说，很难预测哪些物体会穿透哪些表面，会传递多少力。我们可以了解到各种杀伤力较小的弹药的动能（以焦耳为单位），也可以了解到各种头盔所依据的认证标准—— 但很难根据这些信息得出可靠的结论。简而言之，经认证的非防弹头盔所能抵御的动能大大低于低致命性武器可能带来的动能。

头盔可以降低风险。它们不会使风险完全消失。

[image]

挑选头盔

头盔有各种尺寸，每个厂家采用的尺寸模式也不同。在选购头盔之前，不妨先拿卷尺测量一下自己的头围，尤其是在网上购买的时候。如果您没有软的卷尺，可以用一根绳子，然后测量绳子的长度。

很多头盔都是可以调整的—— 您可以通过增加或移除填充物，或者通过收紧或松开头带来调整头盔。特别是硬帽，虽然并不特别推荐，但它是可以调整的。无论如何，最好还是买一顶适合自己的头盔。

✂

如果您的头围介于两个尺寸之间，可能应该选择较大的那个尺寸；但是要知道，太过宽松的头盔可能会在不方便的时刻滑到错误的位置，甚至挡住您的视线。而且，太松的头盔可能会吸收更少的冲击力，因为外部的冲击力会把头盔的侧面推到您的头上，本质上使头盔本身对您产生冲击。

对于有衬垫的头盔，您会希望它足够紧，以至于要花点力气才能戴上它，但又不能太紧，不能让人感觉很局促。

为了测试战术头盔是否合适，在不戴下巴固定带的情况下，用一定的力气左右摇晃您的头：头盔应该不会移动才行。

头盔的种类

本文将根据头盔的设计方式将头盔分为三个基本类别。

有悬挂式头盔，它在外面使用硬层，里面使用悬挂系统来吸收外部冲击力。这一类包括大多数建筑业使用的硬帽、老式军用头盔和一些攀岩头盔。还有一些防撞头盔，依靠可压碎泡沫材料，通常搭配硬层。这些头盔的设计一般都是假设它们会在撞击时被破坏。

自行车、滑板、滑雪、越野摩托车和摩托车头盔都属于防撞头盔。

以及填充式头盔，这种头盔使用坚硬的外壳和内部不可挤压的填充物来减轻冲击。这包括现代军事和战术头盔、以及一些运动头盔，包括橄榄球、棍网球和曲棍球头盔。

防撞头盔一般可以在单次撞击中提供最大的保护，但是，在一次撞击后就会失去保护能力。

悬挂式头盔轻巧、便宜、耐用，但通常没有侧面冲击的防护等级，整体防护能力一般较差。

建议使用有衬垫的头盔，这种头盔通常是为遭受反复打击而设计的。军人配戴这种头盔是有原因的。

悬挂式头盔

悬挂式头盔的优点是价格便宜，而且可以让空气在头部流动，但一般来说，对于钝性撞击的效果较差。一般情况下不推荐使用。

硬帽

首先，也是最常见的，就是硬帽。大多数硬帽可以保护头部不受坠落物的伤害，但对于减轻其他威胁却没有那么有用。

许多硬帽甚至没有下巴绑带，这使得它们在可能涉及奔跑、摔倒或被拘捕的情况下不可靠。工作场所已经越来越多地用“安全头盔”取代硬帽，有些使用悬挂式，有些使用填充物，有些则是混合使用。

如果您要使用硬帽，请寻找“II型”头盔，它包括侧面的非可挤压填充物，并可承受侧面冲击和顶部冲击。这种头盔不多见。

硬帽有一个非常“平民”的外观，在抗议活动中这可能是很有用的，它不会让您脱颖而出。

[image] 硬帽头盔

攀岩头盔

攀岩头盔类似于“II型”硬帽，因为它们的额定冲击力包括侧面冲击和顶部冲击，其位置也比硬帽更接近头部。一般来说，它们更舒适，并提供了更好的流动性。

有传闻说按照欧洲 ASTM F1492 标准测试的攀岩头盔可以有效地防止警棍的击打。

有些攀岩头盔仅仅依靠悬挂系统，而另一些则采用混合系统，结合了填充层。就悬挂式头盔而言，攀岩头盔似乎是一个不错的选择。

[image] 典型的攀岩头盔

古代军用头盔

不幸的是，无法推荐中世纪的头盔或20世纪的钢制战争头盔帮您参加抗议活动，尽管一些抗议者可能会戴上这种头盔。

大多数中世纪的头盔和早期的现代军用头盔使用一个皮革悬挂系统，称为头盔衬垫，以保持硬壳远离头部。

比如复古俱乐（SCA），他们用钢剑和盔甲在抗议活动中战斗，要求钢盔至少是16号或更厚的钢；许多SCA战士喜欢14号钢。任何更薄的东西都可能被认为只是 “装饰性的”。

【注：复古俱乐部 (Society for Creative Anachronism) 是一个国际性的现存历史团体，旨在研究和重建17世纪之前的主要欧洲中世纪文化及其历史。在SCA中经常使用的玩笑将自己描述为一个致力于中世纪的团体。】

我们没有用冲击弹药测试过钢材，但如果头盔被压碎了或变形了，对佩戴者来说是非常危险的。许多SCA战士不是使用传统的悬挂式头盔，而是用½”或更厚的闭孔泡沫建立内衬。其他人则使用现代军用头盔衬垫。

有一些知识指出，与警方使用的那种强大的冲击性弹药相比，古代军用盔甲能抵挡的冲击力要小得多。不论如何，在进行正确的测试之前，不能昧着良心推荐中世纪的头盔。

[image] 2017年9月17日，在圣路易斯，示威者表示反对法院将事实上的有罪不罚扩大到谋杀犯和前圣路易斯警察 Jason Stockley。

有些人戴着早期现代头盔，这种头盔很常见。这些头盔大多没有防弹能力，但旨在保护士兵免受事故和弹片的伤害。少数配有凯夫拉内衬，接近防弹等级的保护程度。

我们很好奇，如果用现代军用填充物和下巴安全绑带取代悬挂式衬垫，会怎么样？但还没有与任何尝试过这种做法的人交谈过。

[image] M1头盔-从第二次世界大战到1985年的美军头盔。

防撞头盔

防撞头盔的种类较多，不容易一一介绍。防撞头盔往往是最容易买到

的头盔，它们通常看起来很“平民”，没有威胁性。戴着自行车头盔的人看起来就像是在下班回家的路上被卷入了抗议人群中。于是，这种装束不会让您看起来像个战士，也就不容易吸引镇压部队的火力。

另外，有些防撞头盔可以隐藏在帽兜下。由于这些原因，以及它们相对便宜的价格，于是可以推荐它们帮助您参加抗议活动—— 尤其是滑板头盔。

防撞头盔不像悬挂式头盔或填充式头盔那样，如果购买二手头盔，效果就不会太理想。幸运的是，它们往往是非常便宜的新产品。

自行车头盔

自行车头盔可能是最不显眼的头盔了，除了像防撞帽这样完全隐蔽的东西，自行车头盔也是可选的。它们的价格也很便宜。这是主要的两个优点。

缺点是自行车头盔的抗穿透能力大大低于其他很多类型的防撞头盔，那种塑料壳太薄了，已经有人亲眼见过警察的警棍把塑料壳完全打碎，碎片飞舞，还划伤了人。

在美国，自行车头盔—— 与滑板头盔和其他运动头盔不同—— 需要使用CPSC标准进行认证。然而，它们只能在一次撞击中幸存下来。简而言之，它们被设计成一次性的。

一项研究表明，几十块钱的自行车头盔与几百块钱的头盔大致一样符合认证标准（基于各种冲击测试）。曾经有FN303弹丸（一种0.68英寸的气枪弹丸）深深地嵌入自行车头盔的泡沫中的案例，这意味着它足以阻止弹丸。

但是，不要忘了，它是一次性的。也就是说，如果选择这种，必须买全新的。

[image] 自行车头盔

滑板头盔和滑雪头盔

滑板头盔比自行车头盔覆盖了更多的头部面积，因为它们的设计不是为了空气动力学的。滑雪头盔在功能上与滑板头盔相同，主要区别只是它们完全没有通风孔，因为它们的设计是为了保持热量。

滑板头盔与自行车头盔不同，不需要认证就可以销售。有些公司显然只认证某些尺寸的头盔，因为他们在不同尺寸的头盔中使用不同数量的填充物。如果通过认证，这些头盔就会被认证为 ASTM F1492 标准，达到比自行车头盔更高的标准，因为它们的额定值可以经受多次撞击。

有些单板滑雪头盔内置通讯系统，这对抗议者来说可能很有用。

滑板头盔是头盔的最佳廉价选择之一。在网上购买滑板头盔时要小心，因为列表中有时是儿童尺寸的儿童头盔，要看清楚。

2018年，俄勒冈州波特兰市的一名警察故意直接向抗议者的头部发射闪光弹榴弹，当时抗议者 Aaron Cantu 就戴着这种头盔。理论上警察应该向空中发射那种闪光弹，在人群上方爆炸 —— 但是，在实际操作中，警察经常把闪光弹对准抗议者的头部。榴弹穿透了 **Aaron Cantu** 的头盔，直接扎进了他的头盔，击碎了他的部分头骨。最后他活了下来，是头盔救了他一命。

[image] 滑板头盔和滑雪头盔

摩托车头盔

摩托车头盔的设计是为了承受比其他防碰撞头盔更高的冲击力。它们也更贵。如果您是专门为参加抗议活动买头盔，摩托车头盔不一定是最好的选择。然而，如果您手边就有一顶摩托车头盔，那就戴它吧，肯定比没有的好。而如果您骑着摩托车或电动车去参加示威，那么您已经戴着一顶头盔了。

全脸的摩托车和越野车头盔对摩托车事故来说有更好的保护作用，但

是，这并不意味着能很好地转化为在抗议活动中的保护作用。这种头盔比较笨重，一定程度上限制了能见度，而且它们使佩戴面罩或防弹镜更加困难。

四分之三（敞开式）头盔和半头盔对抗议情况更有用，因为它们与面罩和护目镜的兼容性更强。半头盔的价格比其他款式的头盔要便宜很多。

✂

在购买摩托车头盔时，您应该注意：DOT认证不值一提，因为它是一个'自我认证'的安全标准。为了真正的安全，特别是防弹保护，一定要买符合**ECE**或**Snell**安全标准的头盔。

[image] 摩托车头盔

马术头盔

马术头盔类似于滑板头盔，那些通过ASTM标准F1163认证的头盔都要经过马蹄的剧烈撞击测试。这对抗议者来说是好事。

[image] 马术头盔

填充式头盔

悬挂式和碰撞式头盔是以防万一的头盔，但有衬垫的头盔是那些预计会被击中头部的人所佩戴的：运动员、士兵、警察，以及越来越多的示威者。可以将这一类别分为两个子类别：运动头盔和战术头盔。

1、运动头盔

比起其他任何类别的头盔来说，运动头盔是专门为防止钝性冲击而设计的；最近在这方面投入了大量的工程。运动头盔也是二手市场上最容易买到的头盔。不过有些运动头盔的设计方式根本无法与防毒面具和护目镜兼容。

请确保运动头盔的填充物处于良好状态。

曲棍球头盔 ——

曲棍球头盔的设计是为了防止快速移动的曲棍球的打击—— 这种冲击力很像警察使用的冲击性武器。半头盔是比较好的，没有下巴绑带或面罩。曲棍球和棍网球头盔是两种常见且有效的抗议用头盔。

棍网球头盔 ——

棍网球头盔很像曲棍球头盔，但它们更轻，并提供了良好的通风能力、以及良好的周边视野。虽然您可能要去掉面罩和下巴绑带，但棍网球头盔是一个可靠的选择。

白水头盔 ——

白水漂流是一项小众的极限运动，白水头盔类似于其他有衬垫的运动头盔，而不是防撞头盔。虽然我们缺乏对这类头盔的直接体验，但似乎它们可以很好地用于抗议活动。

橄榄球头盔 ——

橄榄球头盔是专门为保护头部不受反复钝性撞击而设计的。一些橄榄球头盔采用了双壳系统，利用一家公司所谓的 “防震罩”，内壳和外壳之间的塑料减震器吸收冲击力。显然，这可以极大地提高这些头盔对脑震荡的防御作用。不过，这种技术似乎还没有被广泛采用。

棒球头盔 ——

棒球头盔便宜又结实。传统型号的设计可以承受70英里/小时的棒球冲击，而新型号的额定冲击速度可达90或100英里/小时。美国职业棒球联盟的官方头盔——

Rawlings S100 Pro Comp—— 采用了这种较新的设计，尽管一些球员抱怨它的机动性不如老款。

没有测试过这种头盔与呼吸器的配合情况—— 而且许多这类头盔没有使用任何类型的下巴绑带，因此它们很容易脱落或在冲突中被抢走。

[image] 各种运动头盔

2、战术头盔

战术头盔是为战斗而设计的。这就是为什么警察使用它们的原因：警察是一支占领性的军事力量。

战术头盔旨在保护士兵和其他职业战士免受其工作中出现的危险，如子弹和弹片。

许多这类头盔还被设计成可兼容其他小工具。小工具是有用的：特别是，抗议活动中的活动家可能对能够佩戴耳罩或面罩感兴趣。

记者可能会对安装摄像机的能力感兴趣。尽管无法建议任何人都去拍摄抗议活动，因为这样做可能会使其他抗议者受到伤害。

题外一下 ……

[image]

返回：[image]如何安全地留住证据：给真相的记录者一些技术技巧建议

返回：[image]给公民记录者的技巧指南

返回：[image]公民取证技巧：如何留住真相？

返回：[image]当你手握真相：最基本的防护知识

关于安全购买战术头盔的注意事项—— 很多战术装备制造商都明确地在政治上反对各种抗议运动，而且很多制造商还向警察组织捐钱。虽然有时有必要让资本家把绳子卖给我们来绞杀他们，但值得考虑的是，您的钱去了哪里—— 当您从制造商那里购买时，您会给他们什么信息。您的身份信息也有可能在这种情况下被暴露。

BACK **[image]** 匿名购买

此外，比如在美国，被判犯有暴力重罪的人拥有防弹衣是非法的。除非特殊工作场所的例外。在这里，这项法律可能也适用于防弹头盔。所以，先了解您所在国家的法律。

战术头盔可以通过其防弹等级、风格以及是否设计为可携带装备来区分。它们的价格和功能组合的范围很广。因此，我们将讨论可以混合和匹配的不同类别功能、而不是相互排斥的战术头盔类型。

弹道学

战术头盔有四个等级。最低端的是气枪头盔，通常也比较便宜。这类头盔一般根本没有认证，从功能上看，它们只是较高质量头盔的塑料复制品。

下一种是防撞头盔（与防撞帽不同哦）。防撞头盔是一种战术头盔，虽然它们通常做工精良，并获得了不错的安全头盔标准认证，但它们并不具备防枪弹的等级！它们的重量只有防弹头盔的一半，而且价格也便宜很多。在军队中，这种头盔通常只被那些希望能够容纳像夜视镜这样的装备而没有弹道头盔重量的人使用。急救人员的头盔通常是颜色鲜艳的防撞头盔。

还有就是防弹头盔。几乎所有军用防弹头盔的等级都是**NIJ IIIA ——**也就是说，它们的等级是可以防手枪，但不能防步枪。

最后，还有一些头盔声称可以防步枪子弹。这类头盔大多只能在远距离上防止某些步枪子弹。然而，其他的头盔可以使用一种特殊的衬垫来增加对步枪的保护水平。这也增加了头盔的重量。防弹头盔一般由芳纶纤维制成，如凯夫拉纤维。

对于抗议者来说，您可能面对几乎所有的冲击，最好的一种头盔就是弹道战术头盔。不过，最便宜的新品起步价也在千元以上，大多数好评的型号都超过一千元。

如果防撞头盔，甚至是气枪头盔，能够在不穿透的情况下抵御杀伤力较小的弹药，那么有了防撞衬垫，它们就可以是另一个最好的东西，而价格只有上述的几分之一。不过没有亲测过，您可以亲自测试一下。

风格

以下介绍的是美国型号的防弹头盔。众多用途的款式有很多，但最常见的包括：

1、**PAGST**头盔是一种款式的防弹头盔，自2001年以来已经基本淘汰了。士兵们抱怨说，悬挂系统和垫子不好用，带子效果也不够好。前面的遮挡也限制了能见度，而后颈部的保护延伸得很低，低到足以干扰俯卧位射击。对于抗议者，如果您能找到便宜的**PAGST**头盔，绝对值得佩戴，但如果要掏钱购买防弹头盔，就不要满足于**PAGST**头盔。

2、**MICH/ACH**头盔取代了PAGST型号。ACH是MICH的更现代版本，但两者非常相似。与PAGST相比，它有一个更好的下巴绑带，并依靠填充物而不是悬挂。它被认为可以提供更优异的保护，防止钝性冲击。现在，ECH头盔正在取代ACH；它们的设计非常相似，但它们是由一种更轻的材料制成的，有些人认为这种材料在防弹方面稍弱。这种风格的头盔有 “耳凸”，允许佩戴者在里面戴上耳机，尽管它的贴合度并不总是很完美。

[image] MICH头盔

3、**FAST/ATE/High Cut** 头盔的构造与MICH/ACH头盔类似，但其切口在耳朵上方（ATE），而不是有耳部凸起。这种头盔重量较轻，保护性较低，并且允许使用者佩戴耳罩。如果有选择的话，这可能是最适合抗议现场情况的款式，特别是如果你可能需要佩戴护耳的话。重量只有一半，但可提供同样多的抗冲击能力，尽管对子弹的保护能力较少。这种头盔的老型号，如您可能在二手市场上找到的，有时被称为**CVC**头盔。

侧面防护和护罩

一些弹道头盔 (有时被称为 “仅有外壳”) 是普通头盔，但大多数战术头盔的区别在于其内置的各种安装选项—— 通常是侧防护和护罩。剩余的其他头盔，尤其是老式头盔，如果不带有护栏和护罩，价格就会便宜很多。

“护罩” 是头盔前额上的一个长方形，是用来安装夜视镜的。在民用市场上，大多数人都会用这个位置来安装GoPro相机。护罩是一个相当通用的系统，尽管一些便宜的头盔做工较差，可能无法与配件紧密贴合。

侧防护通常在耳朵上方，有时在耳朵后面，用于安装其他设备。它可以固定面罩、护耳、通讯设备、照明电筒、相机或其他任何你想要的东西。

就像步枪那样，并不是所有的头盔都使用相同的标准来安装侧防护；如果您选择了带有侧防护的头盔，请确保您的配件可以适合它。

在抗议现场，您可能需要侧防护的主要原因是可以安装噪音隔离耳罩。这些耳罩可以掩盖刺激的声音（如枪声、闪光弹、LRAD、烟花和拿着扩音器的自由派等），但可以放大平静的声音。

大多数头盔（不仅仅是ATE头盔）的设计都是可以容纳像头盔下面的耳罩的—— 虽然不那么舒适，但价格可以大大便宜。

如果您需要在战术头盔的前面佩戴任何东西，比如夜视镜，可能需要在后面同时佩戴一些东西作为配重（否则你一跑起来，它就会朝着更重的一边倾斜）。士兵们有时会为此在那里存放多余的电池。

填充物

如果没有良好的衬垫，世界上最坚固的头盔也无法保护您的头部免受钝性冲击。许多头盔，包括一些军用头盔，都没有足够的衬垫。要小心。

衬垫有两个作用：抗冲击和建立一个紧密而舒适的贴合。这两点都很重要。据我们所知，没有一种泡沫能同时满足这两个目的。好的衬垫应该是多层次的。

垫子一般是泡沫包裹在织物中。有时在织物和泡沫之间有塑料，以防止汗水浸透垫子—— 这也很可能是防止化学武器暴露的一个重要特征。有些衬垫将两种类型的泡沫（抗冲击性和舒适性）以多层形式整合在一个衬垫中，而其他头盔则使用单独的衬垫，这使得头盔更加可定制，但也需要更多的工作。在多层衬垫系统中，重要的是在有泡沫的地方都要使用两层衬垫。

所有类型的战术头盔之间的垫子基本上都是可以互换的，因为所有的头盔都使用钩扣式附件，并由佩戴者根据自己独特的头型进行定制。

很便宜就可以找到好的衬垫。任何有信誉的制造商都应该自豪地宣布他们产品的抗冲击认证。

二手

可以在ebay.com或通过各种网站购买二手的头盔。二手头盔总比没有头盔要好，但头盔的防弹纤维会因磨损以及暴露在阳光下时间过久而分解，您无法确定二手头盔的防护性标准。不过，二手头盔还是要便

宜很多。

美国抗议者写的一段话：

> “我的朋友在上高中时失去了一只眼睛。是因为一个警察用橡皮子弹射中了他。几年后，我们参加了新一轮反对警察暴力的抗议活动，每次示威活动都有人严重受伤。我们讨论后得出的结论是：当然，如果我们作为个人保护自己，也许警察会更多地针对我们，但是，如果我们每个人都保护自己，我们整体都会更安全。我的朋友带着满满一购物车的头盔去参加下一次示威，并发表演讲，为人们讲述关于每个人都戴上头盔是多么重要。”
>
> “从那以后，几乎每隔几次活动，就会有人带着一大堆头盔来发放—— 所有不同尺寸的头盔，为大家免费提供，这有助于使佩戴头盔正常化。”

更多相关资料

A Demonstrator’s Guide to Helmets

[image]
[image]

抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

[image] 关键词	护目镜 直接行动 街头 防御 防暴武器 面罩
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月6日
[image] **Description**	行动安全性

保护好自己很重要。我们不需要更多的烈士 —— 我们需要更多可以继续生活和战斗的人。这里是保护眼睛和肺部免受有毒气体和弹丸的危害所需的一切。

- Table of Contents

摘要
1、最贵的
2、更便宜的全脸防护选项
3、更便宜的和模块化的选择
4、赌徒的选择
5、更便宜，但可能不够安全
保护您的肺部，保护您的眼睛
保护您的肺部：呼吸器
1、军用呼吸器（防毒面具）
2、民用呼吸器
附录：**3M**呼吸器**-**分类
半脸的 ——
全脸型 ——
安装呼吸器
过滤器
1、北约螺纹过滤器

2、3M卡口过滤器
更换过滤器
清洁和存放
关于 COVID-19 的注释
防护板和镜片
民用面罩
剩余物资面罩
警察用什么
即兴面罩
DIY面罩
关于面罩的最后说明
保护眼睛
对于那些戴眼镜的人
密封护目镜
弹道学
影响标准
防雾
不建议 您使用以下这些常见的护目镜
一些特定的护目镜，您可以尝试
变通办法

[image]

警察实施暴力镇压的基本方式之一是干扰您的呼吸能力—— 有时还干扰您的视觉能力。如今，无论您是否采用对抗性战术，只要您身处抗议活动”附近”，就很有可能被催泪瓦斯或橡皮子弹击中。甚至不管您是不是抗议者。

通过采取适当的预防性措施，您可以做到减轻风险，将您的行动进行下去。

本集内容将探讨保护眼睛和肺部不受化学制剂伤害和弹丸伤害的多种选择，并详细介绍每种选择的优缺点，以便您可以衡量最适合自己的方案。

摘要

最好的呼吸器是您可以使用的呼吸器。

呼吸器擅长做什么 —— 过滤被污染的空气，大多数呼吸器在紧要关头都能为您提供足够的防护。

如果您没有时间阅读全文，而您又需要赶紧买一些装备，这里有一些选择：

1、最贵的

如果您想买一款新的高质量的全脸面罩，MIRA CM-6M的价格是220–240美元。7M与之类似，但外观更具有 “战术性”。

如果您不想在一次行动中使用价值超过100美元的过滤器，您还可以通过ebay获得两个过期的但未开封的CBRN过滤器，每个大约20美元。这些应该可以适用于催泪瓦斯和胡椒喷雾，但不适用于高级别的威胁。

每个过滤器应该可以工作大约八个小时，也就是在完全的化学品中暴露8小时，这可能意味着30–40小时在街头示威期间，其间涉及大量的催泪瓦斯。一旦您开始闻到有毒气体泄漏的气味，您应该尽快更换过滤器。

如果您戴眼镜，这款面罩与3M安全6878眼镜套件兼容，该套件是为其6800面罩设计的。您将需要为此获得最适当的镜片。

[image] MIRA CM-6M 防毒面具

2、更便宜的全脸防护选项

民用型的全脸呼吸器，如3M品牌6800（150美元，带过滤网），可以以更便宜的价格提供基本相同的保护。在冲击测试中还发现，JJKK和HAOX品牌的中国产品（40美元，带过滤器）同样可以起到保护眼睛的作用，并提供足够的密封性。

[image] 廉价面罩的一个例子

3、更便宜的和模块化的选择

如果您想要一个经济实惠的选择，而且要提供防弹和化学武器防护的最佳组合，您可以花25美元买一个6000系列的3M半脸面罩呼吸器。6100是小号的，6200是中号的，6300是大号的。贴上一对60926的滤芯（一对35美元）。如果面罩自带60921或60923滤芯，就不需要60926滤芯了。另外，买一副 Pyramex V2G Plus 护目镜，价格15美元，用热熔胶封住上面的通风口。如果您戴眼镜，就买RX插片和匹配的镜片。

然而，将半脸面罩与护目镜搭配的最大缺点是，两者之间很难保持良好的密封性，因为护目镜和面罩会在您的鼻子上争夺相同的位置。

[image]

4、赌徒的选择

一个从剩余物资里淘来的俄罗斯军用PMK-3防毒面具有不到20年历史。如果您能找到一个带有全套装备的这种版本，它有弹道镜片和一个用于将其连接到更常见的北约螺纹过滤器系统的适配器。面罩的剩余部分仍然有可能被击中，目前还没有找到关于外挂镜片的防弹等级的具体文件。

如果您想加倍赌一把，俄罗斯的PMK-2可以便宜到25美元，虽然它可能已经有30年历史了。PMK-2可以附带弹道外挂镜片，应该可以用一段时间 —— 但是更换过滤器会很困难。最便宜的面罩直接从俄罗斯发货，运输时间会比较长。

[image] 俄罗斯的PMK3

5、更便宜，但可能不够安全

也许可以假定在多数情况下，您不会被橡皮子弹或催泪弹直接射中脸部。催泪弹会把所有没有防护的人都赶回去，而冲击弹只是偶尔会杀

死或打瞎人。不过很多人都被击中脸部了。处于遭受警察暴力的一端是很危险的。

我们只能推荐具有抗冲击级塑料的眼镜。但如果您没有机会获得这种，而您无论如何都要出去参加抗议，您需要一个全脸防毒面具（军队剩余物资或其他的）或半脸面罩加护目镜。确保您使用的过滤器是军用型的（过期或未过期的），或额定可处理有机蒸汽和P100微粒过滤。确保您的护目镜是密封的。确保所有的东西都紧贴着您的脸。

祝您好运。如果有什么不好的事发生，不要怪我们—— 我们告诉过您不要这样做。

如果您想在您已经获得的东西上进行改进，或者您有不同于上述的战术需求，请继续阅读。

保护您的肺部，保护您的眼睛

我们要解决两个不同的目标：保护肺部和保护眼睛。您可以使用呼吸器来保护您的肺部，过滤空气中的化学物质。您可以使用护目镜、或面罩保护您的眼睛 —— 无论它们是独立于呼吸器的，还是与呼吸器结合成一个全脸系统。

保护您的肺部：呼吸器

呼吸器—— 技术上来说，APR（空气净化呼吸器）—— 是一种在您呼吸空气之前过滤空气中的杂质的设备。

呼吸器或防毒面具有几类，其中有两类我们要完全略过：SCBA (自给式呼吸器)，自带氧气供应，供潜水员和一些应急人员使用；PAPR (动力式供气呼吸器)，通过电力将空气强行通过过滤器，这些都不是行动者需要的。在这里我们将重点讨论全脸呼吸器、半脸面罩呼吸器，以及在较小程度上的一次性呼吸器。我们还将讨论即兴的空气过

滤装备和目前对DIY呼吸器的猜测。

我们将研究两类通用的、非技术性的呼吸器：军用/战术呼吸器和民用/工作场所呼吸器。

1、军用呼吸器（防毒面具）

军用和战术呼吸器主要用于世界各地的军队和军事化警察部队。这些都是全脸式呼吸器 —— 当您听到 “防毒面具” 这个词时就会想到的东西。它们几乎都使用同一种过滤器：北约标准的40毫米螺纹过滤器，有时被称为STANAG过滤器。目前发行的美国军用（可能还有执法部门使用的）面罩配了专有的卡口式安装方式，而不是自封式，使其更容易在现场更换过滤器。

这些防毒面具通常被评为可以抵御从化学武器到核尘埃的全方位威胁。较新的军用型号通常包括一些功能，如语音隔膜，使其更容易让佩戴者彼此对话，过滤器的多个端口允许最大的气流，并使您能够在不移除面罩的情况下更换过滤器，以及供水系统，可以连接到水壶或水囊。

大多数武装部队使用的型号（目前或以前的）都可以接受夹在镜片或面罩外面的弹道镜片或外罩。如果您的面罩可以使用这些东西，您就会想要这些东西。军用防毒面具可以以相当多的钱购买新的，或在二手市场上买到便宜得离谱的同类商品。新的军用或战术面罩起价在200美元以上，大部分在500美元左右。一些剩余物资可以用30–100美元找到。

防毒面具的剩余物资市场是出了名的时好时坏，东西常常被贴错标签。有些东西，比如一些旧的俄罗斯防毒面具，可能是危险的：有些使用玻璃眼罩而不是抗冲击的塑料，而有些可能含有石棉。一定要小心。

下面将列举的是一些常见的剩余物资型号，并讨论它们是否符合现代行动者的需求。发黄的镜片可以修复，但腐烂的橡胶密封圈就不能修复了。老式塑料镜片的抗冲击能力会大大降低—— 在冲击测试中，

只用**BB**弹就击碎了一个以色列防毒面具的镜片。剩余物资的面罩可以从30–500美元不等，这取决于面罩的稀有程度或有用性。足够好的防毒面具（减去防弹等级）似乎一直以80–120美元的价格出售。

[image] STANAG过滤器

2、民用呼吸器

民用/工作场所呼吸器有半脸面罩和全脸面罩两种款式。它们由一些公司制造，其中许多公司使用自己专有的过滤附件。这里将重点介绍3M公司生产的面罩，因为它们的数量最多，而且其他一些公司也采用了他们的 “卡口” 式过滤器安装系统（他们称之为 “滤筒”）。

如果您的面罩已经有了专有的过滤系统，如霍尼韦尔或MSA公司的口罩，请确保您的过滤器的防护等级为**OV**和**P100**。

如果您使用的面罩有专有系统，请继续阅读下文的过滤器部分，以确定哪些过滤器可以适合您。

半脸的 COVID-19 面罩是布制的，但包括呼气阀和可更换的碳过滤器，请注意它不太可能对化学武器有什么用处。它也可能不会保护您周围的人免受病毒的侵害，如果您已经感染了的话，因为它们不会过滤呼出的气。

我们还没有找到任何符合弹道冲击标准的带口罩的民用型全脸呼吸器（下文 “保护眼睛” 部分将讨论），但根据最初的冲击武器测试，3M型号和其他一些型号的呼吸器被评为一般抗冲击性，并且似乎使用与防弹级面罩相同的塑料。一位街头医护人员表示更喜欢佩戴3M 6800全脸呼吸器，理由是它的民用造型比军用造型更容易让患者安心。全脸式民用呼吸器的价格在60–70美元左右，名牌产品更贵。半脸面罩则要便宜得多 —— 仿制品只要8美元，名牌则要30美元。

3M公司生产三种不同型号的半脸面罩和全脸面罩呼吸器。它们中的任何一种都足以满足街头冲突中防护的目的，尽管稍微先进的硅胶面

罩的密封效果更好。很可能7500系列是最适合行动者用途的半脸面罩呼吸器，FF-400系列是最适合行动主义用途的民用全脸呼吸器。FF-400系列配备了语音隔膜，所以您的声音不会听起来那么闷。

3M每款都有三个尺码，但“中号”可以适合**80%-90%**的人。在某种程度上，尺码对舒适度的影响比对功效来说更重要。

eBay上花15美元您可以买一个适配器，从40毫米螺纹过滤器转到卡口过滤器，反之亦然。所以不要单单根据什么过滤器来限制您对面罩的选择。

[image] 3M Ultimate FX全罩式可重复使用呼吸器FF-402

附录：3M呼吸器-分类

半脸的 ——

— 6000系列[基本]：

- 6100: 小
- 6200: 中
- 6300: 大

— 6500系列 [硅橡胶]：

- 6501: 小
- 6502: 中
- 6503: 大

— 7500系列 [硅橡胶，透气性更好]：

- 7501: 小
- 7502: 中
- 7503: 大

全脸型 ——

— 6000系列 [基本]：

- 6700: 小
- 6800: 中
- 6900: 大

— FF-400系列[更高级]：

- FF-401: 小
- FF-402: 中
- FF-403: 大

— 7000系列 [价格明显更高]：

- 7800S-S: 小

- 7800S-M: 中
- 7800S-L: 大

安装呼吸器

无论您戴的是半脸的还是全脸的呼吸器，每次戴上时都要检查是否合适 —— 首先用手挡住呼吸器的滤筒，然后吸气，您应该感觉到在面罩中产生负压，没有空气渗入。然后将手放在出口阀上，然后呼气。应该在面罩中产生正压，没有空气逸出。在进行这项测试时，有些面罩比其他面罩更容易，对于民用面罩，用手去有效地堵住过滤网可能会很困难。

有些工作场所通过将一些气味浓烈的东西或某种温和的刺激性物质放在佩戴者的鼻子下，看看他们的反应如何，来测试是否合适。

虽然有胡子的人已经知道，如果在胡子和橡胶密封圈上涂上大量的凡士林，就会形成一个密封圈。但这种密封很难永久，而且CS粉似乎是脂溶性的，所以它可能会像与皮肤保湿剂和化妆品一样，与凡士林痛苦地混合在一起。一位医生认为，胡子处的化学灼伤可能比把化学品弄到眼睛里更好些。无论如何，剃掉胡须是最安全的选择。即使是几天的胡茬也可能是个问题，需要涂抹凡士林或剃须。

我们采访了一位不想刮胡子的人，他只是觉得空气会有点 “辣”，即使没有适当的密封，仍然觉得自己的面罩非常有用。我们不能推荐这种做法，但可能与您自己的成本效益分析有关。

儿童防毒面具的来源很难。它们是存在的，但生产的数量不一样。MIRA，我们能够找到的唯一一家有库存的供应商，在撰写本报告时已经售罄。有时您也能找到以色列剩余的儿童面罩。MIRA还制作了一个防毒携带袋，可以让用户安全运送婴儿或宠物。

将半脸面罩呼吸器与护目镜搭配使用，最大的缺点是很难同时对两者进行适当的密封。尤其是对于较大的面罩和较大的护目镜来说，更是

如此。第二大缺点是，这样做不能保护脸部所有的皮肤不受化学品的伤害。

过滤器

您需要确保您的过滤器同时适用于油性颗粒物（P100过滤）和有机蒸气。

如果您有一个北约螺纹的军用面罩 —— 对于40毫米螺纹款，您需要CS/CN/P100过滤器，作为一个平民这可能是很难得到的，这些东西通常发给警察；或CBRN过滤器，这是更常见的，但也更昂贵。**CBRN**过滤器对于示威者来说是矫枉过正的，因为它是为了防止化学、生物、辐射和核威胁而设计的。幸运的是，过期但未开封的这类过滤器应该可以在抗议现场使用，而且价格便宜得多。

如果您有一个3M面罩 —— 您需要60921、60923或60926过滤器。

如果您有其他东西，请继续阅读。

如果您很可能会接触到防暴武器，您会希望您的面罩可以过滤两样东西：空气中的微粒和有机蒸汽。

美国的微粒过滤器是根据它们的耐油性来评定的—— N是不耐油，R是有点耐油，P是耐油—— 以及它们过滤掉的空气微粒的百分比 —— 95%、99% 或 99.97%（称为100）。这就解释了N95的名称，即通常用来防护 COVID-19 的口罩。

作为抗议者您要找的是P100，最高级别的保护。这些并没有大幅提高价格，而且似乎没有什么理由使用任何其他颗粒物过滤器，除非您的特定面罩设置只允许N95，这仍然比什么都没有的好。欧洲标准并不对耐油性进行评级，只对颗粒过滤进行评级。P1口罩至少过滤80%的颗粒；P2口罩至少过滤94%的颗粒；P3口罩至少过滤99.95%的颗粒。

虽然常见的催泪瓦斯和胡椒喷雾都是由颗粒物组成的，而不是气体或蒸汽，但空气中的颗粒物本身也会释放出有机蒸汽。您需要微粒过滤器（一般用玻璃纤维纸制成）来阻止微粒，然后是有机蒸汽屏障（一般是活性炭）。**NIOSH**对有机蒸汽防护的认证是 **“OV”——** 请在您的过滤器或其文件上查找。其他一些OV刺激物包括杀虫剂、溶剂和油漆烟雾，所有这些都是口罩在其销售信息中经常提到的。

我们已经看到了基于前线经验的抗议者指南，声称只有OV过滤是必要的。也看到其他指南声称只需要P100。大多数人似乎都同意这是必要的组合，但我们怀疑，在紧急情况下单独一个是否可以。

颗粒物过滤器不会随着时间的推移而降低过滤颗粒物的效果。相反，当它们堵塞到导致呼吸困难时，就有必要更换了。

随着使用时间的推移，有机蒸气过滤器的效果确实会降低，因为木炭变得饱和。热度和湿度都会降低木炭过滤器的有效寿命。热会导致木炭分离，而水蒸气会使木炭饱和，使其无法吸收活性物质。

一旦闻到有化学物质从外面通过过滤器渗入面罩的味道，就应该立即更换有机蒸汽过滤器。

未开封但过期的过滤器一般被认为可以使用—— 只用于有机蒸汽和微粒 —— 只要它们是真空密封的，但如果湿度能够到达木炭，它们很可能已经被毁掉了。多位当过兵的人说过，军方在催泪瓦斯环境中一直使用过期的过滤器，没有任何问题。但这无法确认。

1、北约螺纹过滤器

对于40mm螺纹过滤器，您至少需要 “CS/CN/P100”。AVON、Honeywell 和 MSA 都有生产这种过滤器，但作为平民您很难买到，特别是在冠状病毒大流行期间。

MIRA Safety 公司制造了一种高质量的过滤器；3M公司也制造了这种过滤器。小心从 **ebay** 或二手市场购买**CBRN**过滤器：许多是 **“新”**

的，因为它们没有被使用或打开过，但是几十年前制造的。您需要查找制造日期，否则就是掷骰子了。

对于所有的面罩，您至少需要一个过滤器。有些面罩可以选择一次带两个甚至三个过滤器，以增加气流，对于可能涉及需奔跑或其他剧烈运动的情况，这是一个优势。

2、3M卡口过滤器

3M口罩及其克隆产品使用卡口式过滤器附件。其他一些专有的附件系统类似，但不能与3M互换，但3M是最常见的。如果您使用这些，您很可能最终会使用3M品牌的过滤器。请注意，3M公司区分滤芯（吸收气体的部分，通常由经过各种化学处理的活性炭制成）和过滤器（阻挡颗粒物的部分）。确保您两者都有。您可以通过购买单独的滤芯和过滤器以及连接它们的适配器，或者通过购买预装过滤器的组合滤芯来实现。显然，后者更简单。

向香港的行动者们致敬，他们做了大量的工作，搞清楚了您需要什么滤芯和过滤器。

如果您想要一个组合滤芯，您的选择包括60921（有机蒸汽＋P100），60923（有机蒸汽和酸性气体＋P100），或60926（多气体＋P100）。您需要两个，而且它们通常是成对的。

[image] 两个3M半脸面罩呼吸器，显示了几种过滤器的设置。从左到右：一个p100过滤器连接到带有502适配器的OV滤芯上；一个N95过滤器连接到带有501适配器的OV滤芯上；一个空白卡口连接点；一个p100过滤器直接连接到面罩上。缺失：一体式滤芯，通常可通过亮粉色的外壳识别。

3M公司为他们的P100过滤器打上了霓虹粉色的标记。有些人表示担心这样做会使使用者变得可识别，因为它违反了全黑的行动者美学——不过如果有足够多的人使用粉色过滤器，就不是什么问题了。

[image]

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

更换过滤器

研究表明，在压力下，即使是训练有素的士兵也很难在屏住呼吸的情况下更换过滤器。目前美军型号的面罩—— Avon M50，有自封式卡口安装的滤网，可以让操作者每次更换一个滤网，同时继续通过另一个滤网呼吸。

作为平民，您能接触到的大多数面罩都不会有这个功能。如果要更换过滤器，您可能要屏住呼吸或退出受影响的区域。

波特兰的一位行动者报告说，他们更喜欢带独立微粒过滤器的3M滤芯（6001滤芯带可连接的P100过滤器），因为**P100**过滤器可以在不摘下面罩的情况下进行更换，仅靠滤芯短暂的过滤。

另一位行动者说，他们从2011年开始就一直在使用同一个防毒面具滤芯（军用型40mm的），从来没有通过它尝到过辛辣的空气。这支持了一个理论，即：大部分重要的过滤工作都是由颗粒过滤器来完成的，而颗粒过滤器是永远用不完的，只是堵塞了。

波特兰的其他行动者报告说，他们的过滤器每个都能用30–40小时。

一些多余的面罩采用了位于面罩内部的 “脸颊” 过滤器。更换这些过滤器是一个费力的过程，一些 YouTuber 发现，如果面罩是旧的，那么在更换时很容易撕破面罩的橡胶。

不过，也有人表示喜欢这种面罩，因为他见过警察会抓住其他面罩的外部过滤器让佩戴者无法摆脱，因为脸颊过滤器不容易抓握。

清洁和存放

每次接触化学武器后都应该清洗呼吸器。3M公司有卖这种产品"504呼吸器清洁湿巾"。这些都是负担得起的，但可能没有必要。它们所含的成分是商业机密。大多数人只用肥皂和水，效果一样不错。

不要把过滤器泡在水里，只需用肥皂和水擦拭外面。然后取出滤网，存放在密封袋或其他密封容器中，这样就不会吸收空气中的水分。

关于 **COVID-19** 的注释

与布制的和外科口罩不同，呼吸器并不能保护您周围的人不受您的病菌侵害。然而，比起布质口罩或外科口罩，呼吸器更能保护您自己免受周围细菌的侵害。一名抗议者报告说，他在呼吸器上戴了一个布口罩，以便为其他示威者挡住飞沫。

[image] 反对警察谋杀弗雷迪·格雷（Freddie Gray）的起义期间，2015年巴尔的摩抗议者使用了脸颊过滤的防毒面具。

防护板和镜片

全脸面罩要么使用全脸防护板，要么在眼睛部位使用单独的镜片。镜片在军用型号中比较常见，而防护板在民用型号中比较常见。全脸面罩的可视性更好。有可能全防护板更难做到抗冲击，不过已经找到了两种类型的防弹和非防弹的例子。

带镜片的面罩对于那些要使用武器上的光学系统（如步枪或榴弹发射器上的瞄准镜、红点或铁制瞄准器）的人来说，可以更方便，因为它允许您更好地肩扛武器，并更清楚地观察枪管下的情况。当然，这对示威者来说一般没什么用处。总而言之，全脸面罩似乎更可取。

民用面罩

我们将继续研究非品牌面罩，中国有很多。有些被评为抗冲击；有些使用常见的过滤器样式。到目前为止已经试用了 JJKK 和 HAOX 型

号。在贴合测试中，两者都对我们的脸部形成了足够的密封，尽管还没有将它们带到催泪瓦斯环境中。两者都有抗冲击的面罩，当用各种冲击弹射击它们时，它们的表现与美国品牌**3M**相同—— 也就是说表现得足够好。有人建议购买者应该在 BangGood 或亚马逊购买，而不是在淘宝或eBay上购买这类面罩，因为质量控制稍好。

可以想象，也许可以直接与厂家合作，按照你们所需的规格生产面罩，或者至少是批量采购。有雄心的团体可以考虑在自己的城市或地区尝试这样做。

[image]

剩余物资面罩

剩余物资军用面罩是另一种廉价的全脸防毒面具选择。它们可能很难可靠地找到货源，因为许多零售商（或为零售商服务的其他分销商）在生产日期上撒谎，并可能在功能上撒谎。过滤器也是如此，在ebay上尤其如此。

用于密封的橡胶和用于镜片和防护板的塑料都会随着时间的推移而退化，特别是当暴露在阳光下时；无论是根据我们的测试经验还是从街上收集的轶事，它们似乎都是众所周知的容易破裂。

大多数剩余物资面罩有三种尺寸—— 小号、中号、大号（一般分别编号为1、2、3，编号显示在面罩的橡胶上），但往往网购时无法选择尺寸。

无论您买到什么面罩，都要确保它能紧紧地封住您的脸。即使是劣质的或尺寸不对的面罩，只要它能紧贴面部，并配有足够的过滤器，也能保护您。

如果您能得到正确的型号和原产国，可以搜索在线军事装备网站，交

叉参考卖家的说法。

追踪镜片和面罩的防弹等级一直是个挑战。如果能找到一个接受40毫米北约螺纹过滤器并包括防弹镜片或防护板（通常作为一个单独的外挂附件）的面罩，将会非常有用。对于那些愿意放弃弹道镜片或防护板的人来说，剩余物资面罩往往是最佳选择。

目前美军的主要型号是雅芳M50，250美元就能买到。虽然我们一般不推荐使用专有过滤器的面罩，但M50过滤器相当便宜（目前一对50美元），而且，正如前面提到的那样，您可以在现场更换它们，而不会让自己暴露在有毒气体中。这种面罩的防弹外挂也很便宜。

C50型号是同一面罩的民用型号，虽然它被执法部门广泛使用。主要的区别是，它接受40毫米的北约过滤器。不管是好是坏 —— 通常是更坏 —— 戴上这个面罩会让您看起来很有点像士兵或警察。小心其他抗议者会揍你……

美国军方从1986年到2009年使用的雅芳M40，3M公司生产的民用克隆产品叫 FR-M40，各方面都是一样的。3M公司还为镜片生产了保护性外挂，但我们还不能确定其抗冲击等级。

美国空军和海军自70年代起就开始使用MCU-2P，任何剩余物资都可能是来自该范围内的任何一年，它们在ebay上的价格从150美元到300美元不等。您可以在这里学习如何识别型号和年份。虽然一些文件声称 MCU-2P 防护板是防弹的，但一个特定的防弹罩可以以75美元左右的价格买到。这意味着单单面罩是不防弹的。

俄罗斯的PMK-3（从2000年开始使用到最近，售价70美元）和PMK-4（从2017年开始使用，价格要贵得多）也可以利用防弹外挂，这类外挂往往是全套装备的。全套装备中还包括一个适配器，用于将他们的专有过滤系统连接到北约螺纹系统。PMK-2更便宜 —— 约30美元 —— 通常配有防弹镜片，但只能使用 40mm-GOST 过滤系统（华约国家使用）。

2020年7月，一名《国家地理》杂志的电影制片人在俄勒冈州波特兰

市佩戴捷克**M10**（美国**M17**的仿制品）时，联邦特工用**FN303**气枪的**.68**子弹射中了他的脸，打碎了他的面罩的塑料镜片，严重损害了他的眼睛。这两款面罩都可以选择使用防弹外挂，而他当时没有安装。

以色列国防军使用M15，其民用型号4A1则分发给以色列公民。两者在剩余物资市场上都能买得起。大多数只是标明是作为M15面罩出售，但您可以看出区别，因为**4A1**的眼孔是圆形的，而不是**M15**上使用的奇形眼孔。制造商 Shalon 化学工业公司声称，塑料镜片具有抗冲击性，而且它们似乎没有带防弹外罩出售，但却被一支现代军队使用。

我们还无法确定它们是否被评为防弹级别，所有的塑料镜片都会随着时间和紫外线照射而退化。这两款面罩似乎是最实惠、最容易获得、功能最齐全的剩余物资防毒面具。4A1是我们目前唯一做过冲击测试的面罩 —— 其镜片在受到轻微冲击时很容易碎裂，但不确定受试面罩的生产时间，因为我们买的是剩余物资。

[image] 对以色列4A1进行了冲击测试，结果很令人沮丧

警察用什么

警方使用的装备经常是混搭的，因为他们从军方剩余物资和各种资助机构获得装备。在美国，最常见的两种面罩是 Avon C50（尽管联邦警察有可能使用M50军用版代替）和 MSA Advantage 1000（或其军用级同等产品 MSA Millennium）。人们经常看到C50配备了雅芳面罩通讯装置。目击者报告说，在波特兰看到警察戴着霍尼韦尔北方公司的全脸呼吸器，大概是7600系列。

即兴面罩

一条头巾，最好是湿的，可以过滤掉足够的催泪瓦斯，帮您摆脱困境。这总比没有的好。

有些消息来源说，因为CS会附着在水面上，所以湿的头巾只会让情况变得更糟，但也有其他消息来源、包括真正接触过CS的人都说，湿的头巾可以减少进入呼吸道的微粒数量。有可能湿头巾会变得更早饱和—— 但它会饱和所有的东西，否则那些东西会在您的肺部饱和。

几十年来，抗议者一直在争论湿头巾是否应该浸泡在醋、柠檬汁或其他酸性溶液中。这还没有在实验室里研究过，它的工作机制也不清楚。不过，人们这样做已经有很长一段时间了，实践的人也报告说注意到了不同。**2009**年五角大楼资助的一份报告确实提到，用柠檬汁浸泡的头巾可以减轻催泪瓦斯的影响。

波特兰的抗议者报告说，有些人在使用 COVID-19 防护中常见的较大的面罩，并将面罩拉紧，可能是将拉绳收紧使其高度贴紧脸部。当然，这不是一个完美的密封。一位用户报告说，这种方法可以将催泪瓦斯的效果延迟到许多未戴面具的人被迫离开该地区之后。

DIY面罩

可以制作DIY防毒面具。虽然我们还没有亲自测试过，但 YouTubers 有，并报告了一些成功的经验。我们的想法是用活性炭（过滤有机蒸汽）和棉花（过滤颗粒）来制作DIY过滤器。这些可以连接到任何东西，从重复利用的两升汽水瓶到SCBA面罩。

当然，一个劣质的面罩可能比没用更糟糕。

[image]

关于面罩的最后说明

在多数情况下，您可能不需要一个完美的防毒面具来参加抗议活动。即使镇压部队迅速使用了毒气，就像BLM中那样，通常您需要的只是一些能够保护您足够长时间的呼吸、让您能接近毒气罐并使其失效（盖住它）或将其扔回警方一边。您不需要拥有最高端的装备也能做到这点。

此外戴上呼吸器会很不舒服，特别是在炎热的天气里，因为汗水从您的脸上滚落，紧绷的带子会让您头痛。有些面罩还会限制您的视线或交流能力。呼吸器让您更容易被辨认：即使每个人都戴着面罩，他们戴的面罩也很可能和您的不一样。

但催泪瓦斯的长期影响可能是很显著的，所以保护好自己很重要。我们不需要更多的烈士 —— 我们需要更多可以继续生活和战斗的人。

某些地方和某些时候，警方使用了大量的催泪瓦斯和其他化学武器。在其他地方，他们使用水壶战术或冲击性弹药。

与所有关于您需要安全和有效的决定一样，您需要首先考虑您的地形的具体情况。

[image] 有必要保护您的眼睛免受弹丸和有毒气体的伤害

保护眼睛

同样重要的是保护您的眼睛 —— 免受化学武器和冲击弹药的伤害。

一般来说，这涉及到一个抗冲击等级的全脸呼吸器或一副护目镜和半脸面罩呼吸器。

护目镜应具有防弹冲击 (或至少是抗冲击)、全密封 (无开孔泡沫) 和防雾的等级。不幸的是，这三个方面都是相互作用的，很少能找到同时满足所有这些要求的护目镜。在某些情况下，您可能不得不自己把护目镜上的通风口密封起来。

我们还听到了一些其他值得考虑的建议，比如在普通的、非防弹密封的护目镜上戴上连接在战术头盔上使用的防弹等级的面罩。示威者有

时会戴上棒球面罩和其他运动项目的面罩，但警方使用的许多弹丸都可以通过这种面罩所采用的宽幅格栅。下面这样：

[image]

对于那些戴眼镜的人

如果您近视，不要戴着隐形眼镜进入可能接触化学武器的环境！要戴眼镜。一些喜欢戴矫正镜但又不是绝对需要戴眼镜的人发现，最简单的办法是在戴上防弹和/或防化护目镜的时候把眼镜摘下来。其他人则没有这种选择。对于那些戴眼镜的人来说，也有一些选择，不过这种考虑确实限制了您的选择，增加了护眼的成本。

有OTG（over-the-glasses）护目镜，但我们还没有找到一副能充分密封的护目镜。大多数使用泡沫密封，这相当于不密封。一些行动者知道这点，但不那么在乎。

大多数标准的护目镜，包括那些由 sportsRX 制造的护目镜，都没有防弹等级。我们只发现了一种型号的弹道护目镜—— Wiley X SG-1。目前还不清楚这种款式在眼睛周围建立了多少密封，然而，这是近300美元一副的，也许超出了您的预算。可能还有更好的选择。

许多便宜的防弹护目镜，包括 Pyramex V2G，可以配备插片。V2G 就像我们发现的几乎每一副防弹镜一样，并没有针对化学武器进行密封，但正如下面即将讨论的那样，可以用胶带或热熔胶解决这个问题。大多数全脸呼吸器也可以配备插片，一些抗议者一直在防毒面具中自制眼镜插片，通常使用胶带或吸盘。

一位老兵告诉我们，他在军队时，在向被军队占领的国家的平民分发防毒面具时，他的部队告诉那些戴眼镜的人，把眼镜的柄剪下来，长度刚好能装进面具（或护目镜）的橡胶垫圈内，然后用胶水粘住。热熔胶可能会有用。

另一种样式的 “通用” 方法是将眼镜腿弯曲下来，以适应放入防毒面具的密封圈内。

[image] Pyramex V2G Plus 护目镜

密封护目镜

护目镜有三大类：完全通风、间接通风和不通风（有时称为“密封”）。完全通风的护目镜提供了最好的保护，防止雾气，它们被用于很多运动。对于大多数目的，间接通风护目镜提供了最好的两个世界：通风口允许足够的空气，以保持护目镜不会起雾，并且通风口是足够合理的安全，可以阻挡从化学品飞溅到像锯末之类的粉尘。

不幸的是，这类护目镜无法抵挡催泪瓦斯， 所以对于抗议者来说这不是最佳选择 —— 抗议者要的必须是完全密封的护目镜。密封护目镜完全依靠化学处理和镜片的热传导性来对抗雾气，但这并不总是足够的。

要小心：有时护目镜被列为 “密封”，但却使用开孔泡沫作为密封材料，认为泡沫本身就能向内部通风。开孔泡沫对于涉及警察镇压的情况来说是个坏主意！因为它会吸收化学物质！

另外两种护目镜对脸部形成密封的方法是橡胶和闭孔泡沫。我们没有测试过这两种方法的实际区别。我们的推测是，橡胶密封圈，就像防毒面具的密封圈一样，可以更好地防止化学武器，并且会受到较少的污染，而闭孔泡沫可能会防止吸力问题。

吸力的问题是什么？意思是，如果护目镜以密封的方式（比如泳镜）贴在您的脸上，如果有东西撞到这些护目镜（比如警方用的弹丸），首先，正压可能会损伤您的眼睛，然后，如果空气逸出，负压也会损伤您的眼睛。最坏的情况是，这可能会使您永久失明！

我们研究了一下这个问题，并和一个医生谈过，一般的共识是关于这是否是一个真正的风险 … “也许是”。一些研究表明泳镜会造成瘀伤和一些眼球损伤，这似乎很有可能 —— 虽然我们还没有确认—— 这也解释了为什么泳镜不允许被用于水球等全接触的水上运动。

当然，正如前述医生所指出的，如果您被弹丸射中眼睛，与其说是弹丸击中眼睛的问题，不如说是吸力导致的问题。

据推测，一些自己动手密封通风护目镜的方法可以减轻吸力的危害，因为DIY密封很可能在撞击后失效，使气压正常化。如果这是真的，DIY密封护目镜可能比全密封护目镜更安全。

抗议者一直在采用至少两种策略来密封通风护目镜上的通风口——热熔胶和胶带（最好是贴在通风口的内部和外部两面）。

热熔胶是最理想的，因为大多数胶带在湿润后会失去粘性。布质胶带似乎不能提供足够的密封性，而塑料背胶带则会吸附水分，从而使胶带松动，导致其脱落。只有在紧急情况下才使用胶带。即使是热熔胶有时也会自行松动。

我们还没有测试过其他胶水或环氧树脂。除了热熔胶和胶带，可能还有其他方法。

[image] 用热熔胶密封的护目镜

弹道学

不幸的是，除了向您喷洒化学品外，警察还会向您发射弹药。虽然每一种生产中的冲击性弹药都被特别指定不能射向任何人的脸，但是，镇压部队却经常将弹丸直接射向抗议者的脸。仅在2020年，警察就对美国数十名抗议者的眼睛造成了严重的伤害，许多受害者已经永久失明。他们中的一些人被击中时也是戴着护目镜的。

最安全的可能是找到额定提供“防弹”保护的护眼产品，而不是简单的旨在减轻工作场所危害的“抗冲击性”。虽然这限制了您对护目镜和防毒面具的选择，但如果您知道去哪里找，还是可以找到便宜的防弹眼镜。

诚然，在我们测试不同款式的护目镜对各种冲击的经验中，还没有发现那些只被评为民用抗冲击等级（ANSI Z87.1+）的护目镜和那些被

评为更高标准的 mil-spec（PRF-31013）的护目镜在性能上有任何明显的区别。

我们在测试一副没有评级但被宣传为 “防碎” 的眼镜时也得到了同样的结果。虽然实验还在进行中，但我们目前的假设是，大多数防碎、抗冲击和防弹的塑料镜片的结构是一样的。不过，更高的测试标准也是测试整个护目镜在撞击过程中是否能保持一致，即使是破碎也是如此。

无论如何，某种程度的抗冲击力是至关重要的。我们曾与波多黎各的一位抗议者交谈过，当警察的弹药击中附近的一棵树后，一块大木头碎片掉下来嵌入他们的防弹镜中，他的眼睛最终没事。虽然弹道护目镜的额定值不能承受枪支的直接射击 —— 也不能保证它们能保护您免受各种可能的冲击弹药的伤害 —— 但它们的额定值却超过了胡椒球甚至警棍的威力。在YouTube上，您可以看到人们用猎枪的鸟弹射击弹道护目镜，而不破坏护目镜的演示。

我们测试了未评级的实验室安全护目镜并进行了对比。它们在冲击下危险地碎裂，甚至没有凹陷防碎镜片。

[image] BB弹射击实验室护目镜的结果，碎成了这样。

有些抗议者一直在使用透明胶带来加固护目镜和防毒面具，希望如果弹药打破了塑料，胶带可能会防止碎片分裂的危险，这个前提是基于汽车玻璃的破裂方式。

为了测试这个理论，我们用 Gorilla 胶带 —— 我们能找到的最强的透明胶带—— 只粘住几副护目镜和一个呼吸器上的一个镜片，然后用弹丸射击它们。被胶带粘住的地方穿透力更差，大概是因为胶带困住了弹丸。然而在示威现场，弹丸并不是一个特别现实的威胁。所以我们用**12**口径猎枪的橡胶弹丸射了几颗。有一颗碎裂了，但比那些没有贴胶带的更安全，而有一颗在我们完全预料到会碎裂的情况下根本没有碎裂。这不是结论性的研究，但它显示有可能胶带会有帮助。

[image] 用胶带封住弹道护目镜 [image] 冲击测试后达到ANSI等级的护目镜

影响标准

呼吸器、护目镜和眼镜的塑料(通常是聚碳酸酯)镜片，按不同的抗冲击标准进行评级。在美国，民用护目镜的评级可以达到ANSI Z87.1＋标准，而军用和战术装备的评级则是MIL-PRF-31013或另一个MIL防弹标准；在欧洲，则是EN168A（或者，稍逊一筹的EN168B）。据推测，世界其他地区也有类似的标准。

冲击标准一般是通过以不同的速度向眼镜、护目镜、防护面罩或防毒面具射出BB弹来建立的。要符合标准，镜片必须不破裂或不与镜框分离。大多数 “防弹” 评级要求镜片在每秒至少500英尺（fps）速度的弹丸打击下存活下来。主要的 “抗冲击” 标准，ANSI Z87.1＋，只有150 fps。我们在630和840 fps的速度下射击护目镜，发现两个标准之间没有区别。

一些制造商在他们的销售页面上吹嘘他们所达到的标准，但如果不能做到这一点，它可以是一个很大的工作，以找出什么装备才能抗额定的弹道冲击，特别是关于旧的装备，如剩余物资那种。幸运的是，**ANSI**等级的装备在框架上的某个地方印有**Z87.1**＋，容易识别。

我们不能肯定地说，哪些标准对于防范哪些特定威胁是必要的，因为这些标准在设计时考虑的是工作场所的危险性 (民用型号) 和弹片 (军用型号)，而不是抗议现场会遇到的那种撞击性弹药。我们与工程师们进行了交流，他们建议测试比应用抽象的数学更重要，因为冲击角度、距离、材料的磨损和面罩的形状，都是决定什么会和什么不会打破特定塑料片的重要因素。

无论如何，佩戴防撞护目镜将大大降低对眼睛、脸部或头骨的潜在伤害，即使它真的在撞击时破裂。

防雾

眼镜和护目镜会起雾，特别是在潮湿的环境中。雾状的护目镜很烦人，而且在抗议现场的情况下，有潜在的危险。制造商（和抗议者）

采用了三种基本的防雾措施。

首先，也是最有效的是气流。设计用于对抗雾气的全脸呼吸器在您吸入新鲜空气之前将新鲜空气引导到面罩上，同时确保呼出的空气能立即从阀门中排出。通风护目镜 —— 不推荐使用—— 也是依靠新鲜空气来对抗雾气的。密封式护目镜则在此呈现出劣势。

第二种最有效的防雾措施是使用 “热镜片” 或 “双镜片”，这类镜片之间有一个空气间隙，形成了一个热断层，减少了镜片上的冷凝水。

最后，最常见的防雾措施是在护目镜内侧采用了一个疏水面。大多数号称 “防雾” 的护目镜都采用这种方法，即 在镜片内侧涂上一层薄薄的油。油是疏水性的，所以湿气水珠就会落下来。大多数这些防雾涂层的主要弱点是它们最终会磨损，尤其是在用肥皂水清洗镜片的情况下。一些制造商宣称他们的防雾涂层是以化学方式粘合在塑料上的，不会降解，但我们还没有亲自测试他们的说法。

一位研究者生活在一个整个夏天湿度都在80–90%左右徘徊的地区。在这种条件下，依靠普通的疏水防雾涂层是远远不够的，即使使用通风护目镜，护目镜也会很快起雾。相比之下，间接通风散热护目镜可以佩戴数小时不起雾。这两种方法的差别是很大的。

防雾喷剂是可以买到的，而且价格也相当便宜，不过DIY解决方案也同样常见。许多游泳爱好者宣称用唾液作为薄薄的涂层涂在泳镜内侧，可以防止雾气，而其他人则使用婴儿洗发水（不是成人洗发水！否则会刺激佩戴者的眼睛）。我们咨询了一位长距离游泳者，他报告说，婴儿洗发水在海里可以有效地持续几个小时不起雾，而唾液似乎最多可以持续10到45分钟。

波特兰的抗议者提交了以下防雾配方，我们没有亲自测试过：

材料：牙膏/小苏打，水，*Dawn*防油污洗碗液，强生婴儿洗发水，喷雾瓶（差不多的都可以）。

如果您的镜片有防雾涂层，请用清水和软抹布清洗并晾干。如果您的

护目镜没有防雾涂层：

- 洗好手。
- 使用非美白和非凝胶的牙膏，或小苏打和水。将其涂抹在整个镜片和护目镜/面罩内的裙边上。
- 用手指或软毛刷擦洗镜片，然后用清水彻底冲洗。
- 如果您的护目镜变脏或油腻，请再次重复此步骤。

接下来，混合防雾液：

- 用一个干净的喷雾瓶
- 加入*40%*的防油污洗碗液、*50%*的婴儿洗发水和*10%*的温水
- 充分混合

最后，处理护目镜/面罩：

- 洗干净手
- 将溶液喷洒在面罩/护目镜内侧
- 用干净的手指涂匀
- 静置*30*秒
- 用温水简单冲洗一下，一定要在镜片上留下一层淡淡的溶液，然后让它干燥

- 如果戴上护目镜时觉得刺眼，下一批制作时少用洗碗液，换成水

- 每次行动前都要重复这一步骤

不建议 您使用以下这些常见的护目镜

- 工作护目镜—— 有些带防弹镜片的工作护目镜还配有带子，可以变成抗议行动中的护目镜。但我们研究过的三款这种护目镜都没有真正在眼睛周围形成密封。

- 消防护目镜—— 消防护目镜是为野外消防员设计的，但往往会使用厚厚的开孔泡沫作为通风材料。这样做的目的是为了过滤烟雾，但不会过滤催泪瓦斯。

- 游泳护目镜 —— 游泳护目镜的优点是体积小，密封性好，所以可以和半脸面罩呼吸器搭配使用。但是，很难找到抗冲击的泳镜，值得考虑的是潜在的吸力问题。

- 滑雪镜—— 大多数滑雪镜使用开孔泡沫，而不是橡胶来形成密封。如上所述，开孔泡沫会吸收化学物品。

一些特定的护目镜，您可以尝试

没有完全经过测试，这些建议是基于研究和对话的结合。

到目前为止，头号推荐是 Pyramex V2G Plus。这些都是不到20美元的，防弹等级的，并使用双镜片防雾 —— 一个更可靠的防雾措施。对于戴眼镜的人来说，有一个插片。不过这些护目镜是间接通风的，所以您得用热熔胶或胶带密封它。

唯一潜在的问题是，双镜片的热系统使其更难充分密封。镜片之间有一层薄薄的泡沫，允许水分通过，如果您生活在非常潮湿的环境中，可能会永久地将水分困在镜片之间。

另一个选择是 Pyramex Capstone。也是不到20美元，而且是防弹级别的。它们使用常规的疏水防雾。像 V2G Plus 一样，它们是间接通风的，所以您需要自己密封它们。

SolidWork 安全护目镜价格稍贵，30美元左右。它们使用的是大面积的橡胶密封圈，看起来更能够牢牢地密封在脸上。这些也是间接通风的，所以您需要自己密封。

还有其他很多的护目镜可以用，有防护几乎总是比没有的好。

变通办法

与我们交谈的一个人在通风防弹护目镜下佩戴泳镜。尽管搭配了半脸面罩呼吸器，但泳镜仍能提供了良好的密封性。对于那些拥有专业泳镜或愿意购买一副泳镜的人来说，这种方法也是可行的。

戴起来比较麻烦，估计也不会舒服，而且不知道在化学武器的重重考验下，它的作用如何。如果您有这方面的经验，欢迎留言探讨。

[image]
[image]

如何处理枪伤：街头实战指南 S05E04

[image] 关键词	救助 枪击 直接行动 街头 街头医疗
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月7日
[image] **Description**	行动安全性

您能做的大部分工作都是在开枪之前进行的。请切记这点。

- Table of Contents

  什么是枪伤？
  注意局势和地形
  做好准备
  1、街头医务人员
  2、行动前
  3、装备
  如果发生枪击事件
  即时治疗方案
  疏散
  在医院
  回到家里
  心理创伤
  附录一：个人叙事
  自叙 **1**：生与死的界限
  自叙 **2**：枪声之后
  附录二：额外资源
  附录三：使用止血带的简要步骤

附录四：建立个人急救箱（IFAK）

[image]

示威活动中的枪伤越来越常见。这并不是说您应该惊慌失措 —— 每年全世界都有无数人参加示威活动，去年的镇压如此严重，也只有几十人被枪击。但是，随着政治冲突的升级，行动者还是应该思考如何才能互相照顾和保护。

好消息是，即使您没有受过医学训练，也可以做一些事来最大限度地提高在您附近被枪击的人存活的可能性 —— 只需一些很简单的事。尽管考虑这个问题可能会让人感到紧张，但以下指南可能会帮您有能力帮助拯救生命。

[image]

返回：[image]如何在大规模枪击案中幸存：反侦基础课 S06E09 您首先应该做的是尽可能躲开子弹

[image]

返回：

什么是枪伤？

枪伤包括外伤和严重的穿透伤。它们对身体的影响因武器的类型、射击者的距离、和伤口的位置而异。根据子弹的大小和速度，枪击可以造成不同类型的伤害 —— 包括严重出血、肌肉和骨骼损伤、以及器官的破坏。它们可以以不可预知的方式损害身体。

一些口径的弹药可能直接穿透人体，留下容易辨认的进出伤口，被称为穿透伤，而其他口径的弹药则更容易在体内“翻滚”或弹跳，这可能会造成更多的内部损伤。更糟糕的是，一些类型的手枪“自卫”弹药被设计成在撞击时“爆发”出来，造成更严重的伤害。

无论细节如何，都要将任何枪伤作为潜在的生命危险对待。如果动脉受损，人在三分钟内就会失血过多。一旦一个人失去了一半的血液，此人的生存机会就会急剧下降。这取决于您是否迅速采取行动。

[image]

注意局势和地形

首先，要注意您周围发生的事。

街头示威可能会很混乱和吵闹。警察可能会使用催泪瓦斯、闪光弹、LRAD（长距离扬声装置，即 声炮）和其他嘈杂的武器，而抗议者有时会燃放烟花 —— 这听起来很像枪声。

您在街上被巨大的爆炸声吓到时，请试着辨别爆炸声的来源以及它所代表的风险。

留意任何公开携带枪支的人的位置，以及任何您有理由相信可能携带暗器的人。

在示威活动中，有人被友军的火力击中，也有人被敌军的火力击中。如果您与一个亲密团队，您可以指定一个人留意潜在的威胁 —— 也就是您的亲密团队角色分工，具体方法见下面。

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

您的队友可以轮流担任这个角色，这样一个人就不会因为不断地保持警惕而疲惫不堪。在任何情况下，各方都应该保持警觉，因为事情可能会瞬息万变。

沟通要清晰简洁，特别是当您在描述拥有枪支的个人时。这可以帮助其他人在紧急情况下迅速做出明智的决定，而不会造成不必要的恐慌。

以下是您可以采用的两种沟通模式来传达您所看到的情况：

1、使用 “S.A.L.U.T.E.” (即：规模、活动、地点、单位、时间、装备)来识别潜在的威胁。例如，您可以报告说：“我看到三个人（S）守卫在大街和城市大道（L）交叉口的便利店（A）；而不是大喊 “他们有枪！”；可能是民兵（U），这是晚上11点15分（T），其中两个人有长枪，我不知道第三个人有没有枪（E）。”

2、在紧急情况下，或者时间紧迫的时候，您可以使用另一个工具，叫做 “三个D”：方向、距离、位置；例如：“我的1点钟方向有四个不明身份的人拿着步枪，在上一个街区，用望远镜扫描人群。”

做好准备

您能做的大部分救助工作都是在开枪之前进行的。切记这点。

1、街头医务人员

根据抗议活动的类型和行动地点，可能会有医护人员在附近。您可以事先调查一下您所在的地区是否有街头医护人员，他们是否会参加这场抗议活动，以及他们所在的具体位置。

在示威活动期间，人们经常会看到医护人员在人群中转来转去，或驻

扎在边缘地带，他们带着装备，戴着一个红色的十字或类似的徽章，表明他们是医护人员。

如果您认为这可能成为相关问题，您可以直接问他们是否准备好了处理枪伤和其他严重的伤害。许多医务人员都有应对催泪瓦斯、胡椒喷雾和橡皮子弹的经验，以及疲惫、脱水和恐慌的经验。目前应对枪伤的医护人员不太可能足够多。

如果您正在评估当地医护人员接受处理枪伤培训的程度，并了解到他们准备提供的“第一反应”护理，您也可以询问他们是否有能力在急救服务无法到达一个地区的情况下提供较长时间的护理。这可以给您提供重要的信息，让您了解如果行动仍然处于不断升级的情况下，您可能承担的潜在风险指数。

[image] 布什时代的街头医务人员

2、行动前

在去示威现场之前，评估队友们的安全和健康需求 —— 包括获得呼叫紧急服务的能力和意愿，请注意：紧急服务通常由警察陪同。

在有人到达急诊室之前，是否有什么需求应该被解决？如果发生紧急情况或受伤，您希望您的队友首先联系谁？想清楚这些问题，并安排妥当。

除了了解是否有受过训练的医护人员在附近之外，还要确保您知道最近的急诊室的位置 —— 最好是有创伤中心的急诊室。并非所有医院都具备处理危及生命的伤口的能力。如果您不在设有创伤中心的医院附近，至少要知道最近的医院的位置。如果运气好的话，他们应该能够在将受害者转移到准备好处理大规模身体创伤的医院之前稳定受害者的情绪。

3、装备

有几件物品可以随身携带，在发生枪击事件时可以很有用。

考虑购买或制作一个个人急救包（IFAK）随身携带。个人急救包是一个外伤包，里面有必要的救生材料，可以帮助您控制出血和治疗主要伤口。

它通常是一个小袋子，里面装着纱布（普通纱布或止血纱布）、压力敷料、个人防护装备（手套、面罩）和止血带等物品。一位有经验的医护人员整理了一份详尽的清单，列出了IFAK中应该放什么东西以及在哪里可以获得，该清单包含在文末的附录中。

除了个人防护装备可以保护您和您需要帮助的人免受血液传播的病原体或其他传染性疾病的伤害外，所有这些干预工具都有一个共同的目的就是：尽快止血。

纱布是 IFAK 的基本组成部分，但也是至关重要的一部分。当您对伤口直接施压时，它是用来吸收血液的。纱布也可以用来 “包扎” 较大的伤口。

止血纱布是浸渍了矿物质制剂的纱布，有助于血液更快地凝固，这在大出血时至关重要。

压力敷料（也称为以色列绷带、紧急绷带或紧急外伤敷料）是一种弹性包扎材料，附有非粘附性吸收垫和尼龙搭扣或夹子闭合系统。当用手按住伤口不足以止血时，可使用压力绷带对伤口施加较强的持续压力。压力敷料有很多不同的型号，如果您携带它，请确保您知道它的确切工作原理。看在线培训或装备介绍视频都是很好的选择。

止血带是 IFAK 的基石。如果您只携带一种介入工具，请购买优质的止血带。购买止血带时，最好购买专业部门批准的止血带。这些止血带都经过了严格的制造前测试，并经过了实地使用的彻底检验。推荐美军使用的CAT-7止血带。

小心假货! 许多便宜的产品在市场上流通；这些产品可能在压力下失效。您通常可以通过查看有没有工厂印章来识别假货。最后，也是最

明显的一点，2009年以前生产的黑色CAT都是全黑的，而假货以包含白色的部分而闻名。

[image] 上面没有印章的那个是廉价的假货！ [image] 右边的是假货。看出区别了吗？

[image]

良好的做法是行动前将止血带穿在扣子上，形成一个大环，然后穿过腿或胳膊，而不是在需要使用时在紧急情况下再开始穿扣子。

最后，随身携带永久马克笔，以标明止血带的使用时间，或任何第一反应者—— 如街道医务人员或其他救援人员 —— 可能需要知道的其他伤者信息。根据您的肤色，选择能让笔迹醒目的马克笔颜色。

即使当地有训练有素、经验丰富的医护集体，您自己也应该携带一个IFAK、甚至只是一个止血带，也是个不错的主意。在紧急伤员救治的范围内，很多受过正规训练的医护人员会设法先把伤者自己携带的救助装备用在他们本人身上，以便把医护人员自己的专用装备留给那些什么都没带的人。

正因为如此，您一定要将您的IFAK标记清楚，并随身携带。如果做不到这一点，一定要把您的止血带放在容易拿到的地方，放在您的亲密团队中每个人都知道的有标记的明显位置。让您信任的队友知道您的医疗设备的位置，万一发生不测，他们可以帮您。请使这种做法正常化为基本规则。

如果发生枪击事件

在枪击事件发生后，可能会立即发生几件事。

如果警察在附近并进行干预，您有可能会迅速失去对局势的控制。尽管警察普遍缺乏医疗培训，但他们通常会在伤者周围形成警戒线，并可能阻止医生或其他任何人对伤者进行治疗。

[image]

您的队友应该及时向警察施加压力，要求他们为伤者寻求适当的医疗服务。

这种情况的另一面也是可能的 —— 如果局势混乱或被认为是危险的，即使您愿意呼叫紧急服务，救护车也可能不会进入某个地区。警察可能会花很多时间用催泪瓦斯或其他手段清理该地区，然后才会派救护车来 —— 他们甚至可能会阻止救护车接近伤员（BLM中就发生过救护车被警察拦截的情况）。

在这种情况下，根据伤口的严重程度，生存机会将取决于快速的思维和行动。除了你们自己照顾伤员和组织撤离的专业行动之外，你们将没有任何人可以依靠。

请不断评估周围的情况。是否还有枪声响起？该地区是否有交通堵塞？是否有人从您身边跑过，逃离枪手、警察或暴徒流氓？…… 保持自己的冷静敏锐，不要让惊慌、匆忙或不专心造成更多的不幸。

[image] 装有止血带和创伤敷料的小型个人急救包（IFAK）

即时治疗方案

您在这里读到的任何东西都不能代替适当的医疗训练，简单说，您应该亲手尝试练习，才能真正掌握要领。但是，如果您拥有一个IFAK包或止血带，并且对如何为手臂或腿部止血有基本的了解，采取一些行动肯定比什么不做更好。

[image]

如果枪声响起，尽量不要惊慌。首先，要到一个比较安全的地方。在战术紧急伤员救护系统中，第一步是要维护现场的安全，以免您自己也成为伤员。找到可以评估情况的掩体。“掩体” 指的是任何能阻挡您所面对的子弹的东西，这取决于具体情况和武器的口径。考虑一堵砖墙或汽车的引擎盖。

如果您确定有人被枪击，而您又具备提供援助的能力，请确保现场相对安全。如果您能确定这一点，向您的队友传达您打算向被击中的人移动的信号，以便让队友掩护您。

在移动的同时，向伤者提问，以确定如何照顾他们。问伤者："你在哪里中枪的？"、或者干脆问"你叫什么名字？"如果他们回答了这些问题，这将表明他们的呼吸道尚且是正常的，他们是有意识的，您可能会获得足够的信息来开始准备您的救援工作和心态。

您的第一个想法很可能是："好多血啊！"。起初您可能很难确定伤口的具体位置，特别是如果伤者穿着长袖深色衣服的话，血迹会形成一大片的状况。如果您有外伤剪（专门用于快速剪开衣服的特殊剪刀），请迅速暴露出伤口。一般来说，在皮肤层暴露伤势以了解伤口的确切范围和程度是很重要的。

立即对伤口直接施压。理想情况下，您应该使用戴着手套的手和纱布垫（最好是止血纱布），但在紧急情况下，您可以使用T恤、围巾或额外的口罩压住伤口。

如果血液浸透了纱布，可以增加更多的纱布或另一层布，并施加更大的压力。如果用手直接按压仍然无法止血，可使用加压包扎。将无菌吸收垫放在伤口上，并盖在已经贴好的纱布上（千万不要将纱布拿掉，这样会破坏已经开始的凝血功能）。将弹性绷带紧紧缠绕在受伤部位。它应该施加很大的压力，但不足以切断血液循环。

对于危及生命的出血，时间是最重要的。如果伤口明显在手臂或腿上，而且可以看到大量的血，您可以选择立即使用止血带。与用纱布直接按压或使用加压敷料不同，止血带可以止住特定伤口的出血，也切断了肢体的所有远端循环，也就是说，它应该能止住所有离身体中心较远的出血，而不是应用止血带的局部位置。如果将止血带套在衣服上，要迅速检查，确保没有套在口袋里的物品或其他可能阻碍压力的东西上。

许多人都被教导说，使用止血带很可能会导致副作用，因为切断血液循环会引起并发症；事实上，这在许多野外/偏远地区医疗和街头医疗的框架中止血带仍然是常见的措施。并且，从全球战区获得的数据

已经改变了对止血带安全的理解。经过认证的止血带（如**CAT-7**）现在被认为是非常有效和安全的救命设备，很少造成长期损伤或副作用。如果使用得当，它们被认为是适当的第一线干预措施，而不是仅仅作为 “最后的手段”。

随着对抗议活动的威胁模式发生变化 —— 特别是如果街道越来越多地呈现出战斗区的轮廓 —— 基于武装冲突情景的干预模式，如战术战斗伤亡护理框架，将越来越有意义。

[image]

返回：

[image]

要使用止血带，请打开 CAT-7，确保带子穿过扣环，红色尖端指向心脏。然后将止血带尽可能地往上滑，如果伤口明显在膝盖或肘部以下，而且您很容易看到肢体上没有更高位置的伤口，您可以将止血带放在这些关节上方。

一旦就位，确保带子尽可能的紧—— 想想 “棘轮带” 那种状况。如果您能把一根手指伸到带子下面，就说明带子不够紧。转动滑轮，直到血液停止流动。通过夹子把 “带子” 拉上，并在时间带上标记应用的时间。这个过程会对您的对友造成极大的伤害，会很疼，不过很可能会减轻最初的伤势，这取决于伤口的位置。在使用止血带时和事后都要尽可能地与伤者交谈，让伤者保持意识清醒。

在使用止血带之前，您应该先了解止血带要多紧才有效。试着在示范前将其短暂地放在自己的肘部上方，并将其收紧，直到您不再能感觉到手腕处的脉搏。这是一个很好的同理心练习，可以知道您救助的人将会承受什么样的经历。除非您正在治疗实际的伤口，否则永远不要让止血带停留超过几秒钟。

一旦您通过使用直接压力、压力敷料或止血带止住了血，就应立即寻找其他伤口。用戴着手套的手检查身体的各个部位。在检查过程中，要不断查看自己的双手是否有血迹，以便能立即确定身体的哪个部位受伤。如果伤者穿着防水的衣服，一定要脱掉它或检查衣服的内层，

因为防水布料会使血液留在贴近身体的内侧，掩盖大出血状况。如果发现手臂或腿部有大出血，先直接按压、加压包扎或止血带，一旦出血得到控制，再继续检查其他部位。

在身体外侧部位（即 腹股沟韧带附近、臀部、骨盆部位、手臂与肩部连接处的下方、肩部和颈部底部）的出血可以通过 “打包” 伤口来控制，即 对断裂的动脉或静脉直接施压。如果您当时在不安全的地方，或者您没有配备伤口包扎材料，可以暂时用纱布垫直接压住伤口。

[image]

如果您没有配备**IFAK**或止血带，要大声呼叫医护人员。喊出您所在位置的地标，引导他们迅速找到您，以及伤员是否大量出血等关键信息：例如，“我需要医生！我在红色轿车后面—— 有人腿部中枪了!”

在您等待他们到来的时候，用直接的压力来减缓出血。如果出血是毛细血管性的（流速缓慢且均匀，颜色鲜红）或静脉性的（流速稳定，颜色深红），您可以用直接按压来控制出血。如果出血是动脉性的（喷流状或脉搏性流动，颜色鲜红），直接按压是不够的—— 您将不得不在动脉压力点上施压。

如果伤口在腿部，可以考虑在大腿上部，靠近骨盆区域施压 —— 但要小心。如果这个部位也有伤口，可以尝试在右下腹部位施压。如果伤口在手臂上，可以尝试在腋下按压。如果出血在颈部，可以尝试按压颈部的一侧，一般在下颌骨点的下方，记住只在一侧按压！只有在极端紧急的情况下才需要这样做，因为这样做对控制出血的价值有限。

无论伤口在哪里，一旦施压，不要为了检查伤口是否还在流血而取消施压。您必须继续按压，直到医生可以给伤口加压包扎或采取其他止血措施。

如果伤口在胸部，用戴着手套的手捂住伤口是可以接受的，但施加过多的压力可能会抑制伤者的呼吸系统。胸部伤口一般出血较少，但有很大的风险，空气会进入胸腔，导致压力积聚，可能导致肺部塌陷。

有些医护人员在急救包中会携带通风胸封，其作用与戴手套捂住伤口的一般作用相同：防止空气进入胸腔。如果伤口在肢干上—— 即 在胸部和肚脐之间 —— 除了立即通知医护人员或其他更高级别的护理人员外，您可能没什么办法。

如果您能控制出血，您或队友应该让伤者做好准备，以应对可能的急诊就诊或其他可能被没收财产的情况。从受害者的背包、口袋和身上取下任何可能导致伤者被定罪的物品。让队友将这些物品处理掉，或者将它们交给值得信赖的朋友，让朋友将这些物品带离现场。

当更高层次的护理人员到达时，无论是急救中心还是街头医护人员，尽您最大的能力给他们一份报告，使用**MIST**缩写词：受伤机制（**M**），所受伤害（**I**），症状（**S**），以及已经采取的任何治疗（**T**）。例如，“他们在两个街区外被步枪射中，左腿有两处弹伤。他们的皮肤触感冰凉，呼吸似乎比正常人慢。我用止血带高高紧紧地缠着，血似乎已经止住了。”

如果医疗护理需要一段时间才能到达，可以考虑用记号笔在病人的手臂上写下症状或其他您注意到的重要信息。

[image] 可以在皮带上佩戴的小型IFAK，标有十字，方便识别。

疏散

了解您的疏散选择。您是否在警戒线后，以至于救护车无法通过？当地的医疗团体是否提供去医院的交通工具？如果您认为自己处于救护车可以进入的区域，您可以尝试呼叫救护车。

当您拨打急救电话时，您可以要求他们不要派警察来，但他们很可能会忽略您的要求。如果您决定拨打急救电话，而您是在一群人中积极地试图帮助伤者的人，指定一个人拨打急救电话，并报告伤口和位置，而其余的人则专注于帮助受害者。有可能—— 但不保证—— 急救调度员可以指导您完成基本的创伤反应，直到您得到专业的帮助或可以运送伤员。

如果您或您的战友开车去参加示威，如果附近停着一辆车，其位置可以立即进入道路，就会有帮助。确保您知道钥匙在哪，并且可以让一个以上的人获得车钥匙。在发生枪击事件时，其他人很可能希望协助。如果您自己无法运送伤员，请向周围的人寻求帮助。

在医院

在一些城市，医院会将枪击受害者置于保护性监护之下，以消除对他们的暴力威胁。

但如果出现这种情况，您将无法在医院系统内找到您受伤的朋友。如果当事人昏迷不醒，无法告诉医护人员该联系谁，医护人员会尝试联系家人。

[image]

也就是说，如果您进入的环境有可能会受到严重的伤害，您可以在自己的皮肤上用不褪色的信号笔写上一个紧急联系人电话号码，并注明“紧急情况下打这个电话”。

虽然在发生枪击事件时，这可能不是您最重要的想法，但重要的是要知道大多数大型医院系统提供的项目是什么，您可以通过这些项目申请援助。

如果有人命悬一线，您可以要求先救人，在以后解决财务细节问题。

回到家里

当把伤者从医院带回家时，需要评估他们的家庭情况。他们是一个人住吗？还是与朋友或家人住在一起？他们的卧室是否在楼梯上？根据伤势的严重程度和预测的恢复时间，他们可能需要改变自己的生活状况。

在很少有公共卫生系统的国家，人们往往很快就出院了—— 有时在他们应该出院之前就出院了。这可能会让人感到害怕，但好消息是，家庭通常是一个比机构更好的恢复环境。您可以租一张病床，可以推的那种，可以摇动把手让伤者坐起来。普通床不具备这种功能。

如有必要，请组织您的社区护理，以便有人在场或24小时提供服务。即使没有必要，也要试着组织一个由朋友和亲人轮流担任照顾者的轮班时间表，以确保照顾工作不至于完全或大部分落在伤者的伴侣身上。此外，您可以制定一个用餐时间表，让互助小组轮流为伤员和护理人员送去食物和杂货，或为他们做饭。

心理创伤

虽然不用说，不论是您自己被枪击还是帮助被枪击的人、或只是目睹某人被枪击，或您所爱的人被枪击，即使您不在现场，都是一种创伤性事件。您可能会经历一系列的反应，包括噩梦、焦虑、逃跑/僵持/战斗反应、自我怀疑、神经症、恐惧和抑郁。不要孤独一个人，去寻求帮助，形成一个社区关怀圈，每周聚会一次，处理大家的痛苦、困惑和创伤。

如果您的社区中有许多人受到该事件的影响，您可以从您的圈子外寻找朋友或亲人来帮助您处理发生的事。在您所在的城市找一位心理治疗师来帮助您。虽然治疗通常看起来成本很高，但也许可能找到一个非营利组织、诊所系统或大学，在那里接受培训的咨询师可以免费或以优惠价格提供服务。

如果您所在的城市有持续的抗议活动，当地的非营利组织可能会专门为受影响的人提供咨询。此后我们将更详细解释如何做这件事和提供一些工具，可以用来帮助您的社区成员掌握基本的心理救助和互助。

[image]

在反抗者社区中，长期以来有一种模仿强硬态度和虚张声势的倾向。您需要分析和/或克服某些不好的社区文化规范，避免 “被动” 和 “好斗” 之间的二分法，这样才能帮助您建立可持续的长期运动。

请记住，我们要的是一场彻底的革命，而不仅仅是周期性的上街。

[image]

附录一：个人叙事

以下内容来自美国的反抗者，可以帮助您直观地了解在类似情况下的行为。

自叙 1：生与死的界限

这是一个风雨交加的夜晚，这是一周来持续下雨的第一个夜晚。人们在一家烧烤店的遮阳棚下站着，面前吊着警戒线，等着看会发生什么。不止几个人的腰带里塞着枪。有的人与警察扭打在一起，有的人将碎水泥块扔向坦克；有些人在激烈的争论，我们是否应该回家，不要再违反宵禁了，改天再打。然后，突然，一辆孤零零的警车从后面吱吱喳喳地驶来，警笛声响起。

人群四散，人们惊慌失措，四散奔逃，催泪弹在街上横冲直撞，闪光弹榴弹在警戒线上爆炸。到处都是呛人的烟雾、混乱和恐惧。枪声响起，有人穿过人群向那辆孤零零的警车开火，警车已经转身撤退。我在一个蓝色的邮筒旁，迷茫地与朋友们分开了。人潮顺着街道流向远离警戒线的地方，警察开始推着人群前行，想要疏通人群。被卷入人海中，我沿着人行道走了大概二十步，才看到一群人结结实实地围着躺在地上的一个人。

时间慢了下来。我的两个好友正围着人行道上的一个伤者。那个伤者是我最老最亲的朋友之一。

有人在尖叫："他中枪了，他中枪了！"我的一个朋友正在喊着让人们后退，当他抬起头来看到我的时候。我看向地上的朋友，他的腿部中弹了。但他的眼睛里的光芒正在逐渐消失，他抱着自己的躯体呻吟着。

我们很困惑，没有血，没有血。到底发生了什么？他伤在哪里？没有血，只是从他嘴里发出一连串令人难忘的呻吟。我是一个母亲，我知道在生与死的分界线上的人听起来是什么样子的，在这绝望和迷茫的时刻，我只知道这个我深爱的人正悲惨地躺在我面前。

我还是不知道到底发生了什么事，但我知道我们必须尽快救人！

没有人会来帮助我们，也没有人会来救他。我跑向我的车，谢天谢地，我的车就停在几个街区之外。我飞快地绕过街上尖叫的汽车。当我回来的时候，我发现人们把我朋友抬到一辆已经挤满了人的车里。我尖叫着说他要和我一起走，我的朋友们把他从那些好心的陌生人手中抢了过来。我们沿着街道奔跑，我知道我想去哪家医院，但天黑了，我很困惑。其他队友把车停在我们旁边，问我们是否需要被带到医院。

当我们到了医院，把我的朋友从车里拉出来的时候，他的衣服滑了下来，我才真的看清楚：那里就是入口伤，但没有出口伤（不是贯穿枪伤，子弹留在体内了）。他立即被转到了创伤医院。在接下来的日子里，我们不断听到 “可能已经死了” 这句话。

在这之前我都不知道中枪是什么意思，中枪意味着什么，就是子弹撕裂了肌肉，也许穿透了骨头，也许摧毁了一些器官 —— 很可能是一些重要的器官。它可能摧毁左肾或脾脏；它可能使两肺塌陷，夹在食道上，在体内出血时，血液会填满内腔。一颗子弹可能最终打进心脏。你可能会在半夜的医院里被一个很有耐心、很善良的心脏科医生哄着看一系列的法律文件，他正准备给你爱的人做第二次开膛破肚的手术，捞出那颗扎在他心脏里的子弹。

那天晚上，运气是站在我们这边的，绝对是这样。但我们对枪伤情况的反应也足够快。后来我发现，很多不同的朋友都这样做了，我不是唯一一个跑去找车的人 —— 我只是先到了那里。而好心的陌生人正试图帮助疏散—— 在这个城市里有很多人被枪杀，人们都知道自己在看什么，以及快速做出正确的反应是多么重要。

我朋友的遭遇并没有阻止我重返街头，也没有阻止他或我的社区的其他人。因为医院把我的朋友置于保护性监护之下，只有我和另外一个

朋友能探望他。我的许多朋友在继续肆虐的街头战斗中寻求安慰，很高兴看到他们有机会将他们的悲伤、恐惧、绝望和愤怒转化为行动。

我很庆幸，那晚我恰好就在附近。我很庆幸，身边有那么多人想帮忙。我很感谢人们意识到我们需要他们带我们去医院。我很感谢转到创伤中心的过程足够快，我很感谢善良的外科医生。我很感谢我的朋友内心的意志足够强大，他活了下来。我很庆幸他活了下来。

你们也可以做一些事，做一些准备，当你发现自己遇到类似情况时，可以尽可能让事情变得好起来。

我也感谢抗议现场的紧急救助小组。如果你需要他们，愿他们在你身边。

自叙 2：枪声之后

我们都听了。一声枪响。它响彻了整个夜晚，在几个小时的相对安静的打斗和激动的人群的沙沙声之后，它奇异地出现了。

广场上有数百人—— 许多人排队想进入活动现场，也可能有同等数量的人试图阻止他们。帽子像短程烟花一样在人群上空飞舞，人们抢着扔帽子。这是一场混乱，鸡蛋、油漆弹、胡椒喷雾和拳头，从各种奇异的角度和四面八方涌来。为数不多的警察在现场并没有介入。从广场上退到黑暗的校园街道上，整个局面看起来就像一部低预算剧中导演拙劣的打斗场景。

但我们都听到了那声爆响。只是那一声。本能地，黑衣人群整个散开了，人们都抬起头来。鉴于我们到那时为止对示威活动中发生的事的了解，我们以为那是一颗闪光弹榴弹。那是我们认为唯一能发出这种声音的东西。但没有第二声爆炸。每个人的目光都重新聚焦在周围的僵局上。推推搡搡，一些加固的横幅和手机被抢走，但相对平静。

抬头看向广场对面，我瞥见了一些不对劲的地方。那是一个我认识的人，一个我知道的敏感人士。他一直在努力确保不会有人受伤，但现

在有些不对劲，无法判断是什么。

我和一位队友穿过人群，被推搡着到了他所在的地方。空气中弥漫着各种气味，不是单一的味道，空气中的烟雾还有一种金属的味道。当我们到达他身边时，他脸上的表情告诉我，他已经很危险了，还有那声音，他发出了一种你肯定不会发出的声音。尖叫声和咕噜声混合在一起。我不知道他怎么还能站着。我先到了他身边，他靠在我身上，虚软无力。他的皮夹克的味道，以及他在那绝望的一瞬间压在我瘦小的身躯上的重量，是多年后一直在进入我的梦境、让我惊醒的东西之一。我仿佛背负着一具死尸，但似乎仍是活的。

他直直地盯着我，却又穿透我的身体。我意识到他快死了。但我不知道为什么。各种原因在我脑海里闪过，几乎没有血迹，我也找不到任何东西。我们并没有走那么远，最多也就二十英尺，而我能想到的最大的可能性就是他一定是撞到了头，只有头部受伤才会让他这样语无伦次。

然后医护人员就把他带走了，我们从那一刻起就没有了联系。我盯着医护人员，幸好我信任他，我只能说出 “他受伤了，我不知道伤在哪里” 之类的话。除了把他从眼前的危险中救出来，我觉得自己完全没用了。

医护人员开始做着自己的工作，现在可以看到有不少血迹的地面上。我听到人群中传来低沉的喧哗声—— 那是当你快要晕倒时发生的时候能听到的东西，隧道尽头的声音。

有人开枪射中了他。

警察突然冲进去把他带走了，把那些训练有素的外伤医护人员强行拉走，我们都在警戒线的另一边尖叫。现在大家都知道他快死了，出事了。我想喊 “他中枪了”；我开始喊，但后来我意识到这可能会引起人们的恐慌。我只是勉强意识到自己已经很恐慌了。我找到了一名医护人员；他们确认有人向他开枪。

警察把伤者装进了某种没有顶的车辆的后面，就像校园警察用的那种

车。示威还在继续。找到我的队友要求我们离开，“他们/警察” 在向我们开枪，我们必须离开。但那时候，我甚至不知道威胁来自哪里，也不知道离开是否能更安全 …… 我们在那个犯罪现场呆了几个小时之久。

附录二：额外资源

1、《像世界正在死亡一样生活》播客播出了对一位经验丰富的街头医生的采访，他对如何在示威活动中应对枪伤做了详细的说明。

2、在另一个播客中，在2017年1月20日的示威活动中被法西斯分子枪击后幸存下来的 Hex 讨论了正义、暴力、父权制和同情心、治疗的关键，以及如何重新定义抵抗。

[image]

返回：[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06

[image] 1970年5月15日，身穿防暴服的警察在28秒内发射了150多发子弹，在密西西比州的杰克逊州立大学谋杀了两名年轻的黑人，并打伤了十多人。尽管几天前在肯特州的谋杀案仍广为人知，但随后在杰克逊和乔治亚州奥古斯塔的年轻黑人示威者被谋杀案却常常被人遗忘。

附录三：使用止血带的简要步骤

- 找出伤口的位置。

- 使用止血带，如果伤口明显在手臂或腿上，并且您可以看到大量的血，则在衣服上使用止血带。

- 确保红色尖端指向心脏。将止血带尽量放高。如果伤口在膝盖

或肘部以下，将止血带放在关节上方。

- 拉紧尾部。尽量拉紧带子。
- 转动滑轮，直到血流停止。
- 记下使用止血带的时间。
- 继续与您正在治疗的伤者交谈，让伤者保持清醒。

附录四：建立个人急救箱（IFAK）

- CAT Gen 7 1个
- 紧急创伤敷料（ETD）2个
- 胸封贴片 2个
- 止血纱布 1包
- 永久信号笔 2支
- 丁腈橡胶检查手套 2副
- 不锈钢剪刀 1把 剪开衣服

希望您和您的队友永远不要碰到这种情况；但是，如果不幸遇到枪伤，您可以采取最及时的最佳措施，以缓解伤势并坚持到救护车到

来。

[image]
[image]

从雨伞到激光、气球到电动工具：街头实战指南 S05E05 - 战术器具综述

[image] 关键词	亲密团队 安全文化 直接行动 街头 街头战术 防御
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年1月8日
[image] **Description**	行动安全性

“待在一起，紧紧地靠在一起，我们每天晚上都这样做” ——
记住这句歌谣，和大群人紧贴在一起也是一种很有效的战术。

- Table of Contents

I 数字安全
II 掩饰和正确的着装
下面是更多细节：
III 后勤
IV 鼓风机
V 伞
VI 盾牌
VII 体育器材
VIII 气球和泡泡
IX 激光器
X 涂鸦
XI 漆弹
XII 焰火
XIII 火

XIV 推倒围栏
XV 解除逮捕
XVI 群众运动
XVII 阻止摄像头，破坏窗子
XVIII 法律协助，监狱协助

[image]

在去年两个多月的抗议活动中，波特兰的示威者尝试了各种战术和战略。

从6月中旬开始，波特兰的冲突就引起了国际社会的关注，当时传出联邦探员开着没有标记的汽车将示威者从人行道上强行绑架的画面，特朗普宣布，联邦探员将使用这种模式镇压美国其他城市的抗议活动。特朗普宣布后，波特兰的示威活动成倍增长，每晚都吸引了数千人，直到俄勒冈州州长宣布联邦特工将撤出街头。

本文将总结波特兰示威活动的参与者描述的他们在那里看到和使用的一些工具和战术。

这些工具中的许多在相互结合使用的情况下效果会最好。一如既往，战术的多样性是关键 —— 不仅仅是接受不同的方法，更多是要思考如何将所有这些方法结合成一个共生的整体。

波特兰的抗议活动也产生了一些新的术语，比如 “**swoop**” 这个说法，它描述的是当一个拿着扩音器的改良主义者玩弄权术，劫持一群由希望看到彻底变革的人们组织的集会时发生的情况。随着示威者扩大他们对在这个迅速分化的社会中 “什么是适当的战术” 的概念，我们希望他们也将扩大自己对什么是值得为之奋斗的愿景的认识，采用横向的组织模式，并学习如何识别和抵制权力的把戏。

[image]

I 数字安全

本集主题的背景是大型抗议和激进起义现场，所以这里专指行动现场

的数字安全性措施。

包括比如，如何在示威游行中通过适当的手机安全设置来保护您自己的安全—— 在抗议前、抗议中和抗议后，比如这些：

[image]

返回：[image]当您准备参加抗议活动：基本指南

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

返回 - 如果是紧急的前期培训，建议从这里开始：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

以及更多。您可以从本站 “行动安全性” 专题中看到。

但必须说，安全首先是一项心理素养，因为它需要您在突发威胁出现时快速识别并做出尽可能正确的反应，这是需要日常训练的。不论您是培训师还是自主学习者，我们建议您从**S01**开始。

同时，安全也是一项重要的协作能力 —— 没有人能独自实现安全，尤其是在冲突环境下，如果我们不能彼此保护、如果我们不能确保我们的战友坚守安全规则，所有人都会陷入困境。

所以在上场之前，您的准备工作应该 从安全文化开始 ， 作为战术部署的重要环节；并应 致力于培育和滋养您的亲密团队 ， 在关键时刻，你我很可能是彼此最重要的生命力保障。

[image]

返回 - 作为组织基础设施：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

返回 - 作为组织结构：[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南 S05E09

顺便说，对于激进社区和激进行动计划的独立学习者，请从本站 “威胁知识库” 进入相关主题：

[image]

返回：[image]匿名手机 ；[image]生物特征隐藏 ；分身 ；[image]数字技术限制和最佳实践 ；加密 ；[image]元数据擦除和避免 ；[image]防篡改准备

II 掩饰和正确的着装

戴面罩从安全的角度来说是为了保护您自己的隐私。如今您不仅要担心警察的拍摄取证和逮捕，还要担心在线的 **Trolls** 试图从视频画面中识别您的身份导致“人肉”威胁。

[image]

返回：[image]给活动家的反人肉指南

返回：[image]如何知道有人正在线人肉你？6个简单的方法

如果示威者能穿着合适的统一黑色团队服装，应该很难辨别出身份细节。但这需要您首先判断一系列问题，并作出周密的行动计划 。在下面看到具体建议。

[image]

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

不能只关注脸！要注重您的身体上的各种细节！如果您有纹身和其他独特的特征，必须遮住；遮住您的整张脸，不要只是遮住嘴巴——

简单说，您应该选择面罩，而不是仅仅口罩；检查自己的衣服、鞋子或背包上，不应该有任何明显的标志。

下面是更多细节：

1、对您何时何地戴上面罩和穿上匿名衣服，要格外认真；您换衣服的地方不应该有任何监视摄像头存在、也不该有除了您的亲密团队之外的其他人在场。

如有可能，请提前探索可行的更衣区域，以找到合适的更改空间。请记住，警察特别有可能将目标对准蒙面的行动者。

[image]

返回 - 相关自卫主题页面：[image]匿名着装 ；[image]监视器排查 ；周密的行动计划

穿着和携带不同的服装，这样您就可以为可能发生的一切做好准备。

理想情况下，您应该有一套非常普通的衣着，可以在不引起注意的情况下让您抵达行动地点，然后您就可以为行动本身更换匿名装备，把它套在普通衣服的外面，这样当您离开该地区时及时脱掉外面的衣服，让您看起来就像是一个普通路人。

[image]

返回：[image]匿名着装

以及：[image]特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06

不要忘记保持水分，尤其是当天气炎热的情况下。

2、如上所述，如果您有纹身或可见的疤痕，一定要遮盖它们！您可以使用化妆品或遮瑕膏来做到这一点。

许多演员和舞者都使用 Dermablend 遮盖纹身，烧伤和疤痕（这是一种高遮盖力底妆产品）。它具有多种颜色，可以混合以匹配您的肤色，并且具有防水功能，可以持续使用**12**个小时。

这东西比较贵，但是比保释金便宜。如果找不到 Dermablend 或类似产品，请尽可能用衣服围巾或其他东西遮盖纹身和疤痕。

同样的，您的身上有可见的穿孔吗？耳洞、鼻环、唇环等等，把饰物取下来，遮盖穿孔的位置，让它尽可能不明显。

3、请不要穿着与众不同的衣服进入行动团队！

警察可能很愚蠢，但是他们可以将目标人的照片和紫色波点裤与同一个人的相同衣服（不包括面部）的照片进行匹配，瞄准身材特征和习惯性姿势等细节，以识别一个人；即使这些照片是在不同的日子拍摄的，也是如此。

同样的，如果您有背包或其他包，请不要随身携带。无论您的衣服伪装得有多完美，如果您的包可识别，其他所有都是徒劳的 —— 特别是如果像许多人一样，您换包的频率比换衣服的频率要低得多。

出于相同的原因，您的鞋子也同样如此 —— 行动中的穿着与您每天习惯的穿着必须不同！这也很重要，因为警察可以尝试使用鞋子的脚印或其他痕迹作为证据。更多详见：

[image]

返回：痕量证据鉴定

在行动团体中时，您的衣服和背包上不应该佩戴任何标志/胸牌等东西，除非，您的团队中每一个人都佩戴了相同的标志。总之，思考方式是，尽可能让水滴融入一片大海。

4、再次强调，不要仅仅遮住脸！头巾很受欢迎而且很方便，但是掩

饰不够。

您需要完全遮住头部，以免看不见您的头发，尤其是与众不同的头发。

在某些情况下，如果适合您的行动，您可以尝试假发。

如果可能，遮住眼睛。护目镜可以做到这一点，同时具有保护眼睛免受化学武器伤害的双重目的。

[image]

返回 - 在上一集中看到面罩和护目镜的选择方法和使用建议：[image]抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

不起眼的普通的太阳镜也可以在紧要关头起作用。在您可能接触化学武器的情况下，不建议使用隐形眼镜。

5、注意不要留下指纹和**DNA**证据！

戴上手套，事先用酒精湿巾擦拭工具和其他物品，以清除它们上的指纹 —— 您永远不知道可能会在混乱中丢失什么。

不要忘记手电筒内的电池！上面也有您的指纹。

具体内容请从“威胁知识库”进入。

[image]

返回：DNA ；[image]指纹 ；痕量证据鉴定

6、在家练习。

在期望正面迎战警察惊艳的技艺之前，请不要穿您从未穿过的笨重衣服。

您需要熟悉自己的服装、并且穿着舒适，要让它利于激烈动作；同样重要的是，您的视野也不能受到影响。

不要让上述这些保护性措施给您带来虚假的安全感。要随时当心！评估您的状况以诚实地冒险；如果不确定自己是否可能承受最严重的后果，请不要做任何事。

时刻注意周围的环境并倾听自己的直觉。

确保您了解并信任与您一起工作的人员，尤其是在涉及高风险活动时。

始终练习正确的安全操作！了解并维护您的合法权利，尤其是在压力大的情况下。这样做无法百分百确保事情变得更好，但是如果不这样做，百分百肯定会使事情变得更糟。

[image]

请谨记美国活动家 Abbie Hoffman 描述的革命者的首要职责，4个字：不被抓住。

要站着，把事办了。首先有人的安全才有我们未来的一切。

III 后勤

如果能安排一群人提供食物和其他需要的资源，对维护士气真的很有帮助。波特兰的抗议者们已经深深地感谢 Riot Ribs 出来给大家提供免费食物。这使得人们能够停留更长的时间，让行动者感觉到支持滋养他们的运动是值得的，也是值得冒风险的。

□

延伸：https://nodebe4.github.io/oped2/2020-05-11/%E5%A6%82%E4%BD%95%E5%96%82%E9%A5%B1%E6%8A%97%E8%AE%AE%E8%80%85-%E8%B5%B0%E8%BF%9B-%E5%8F%8D%E5%8F%9B%E5%8E%A8%E6%88%BF-iYouPort/

政府和警察知道这些互助努力有多重要，于是镇压会故意针对这些后勤人员，以期借此打击示威者的意志。

不幸的是，穿制服的警察并不是威胁社区基础设施的唯一危险。7月下旬，Riot Ribs 经历了一场涉及身体暴力和恐吓的政变。

[image]

凡是 有金钱参与 的活动，都有很大的内讧风险，除非目标、结构和期望值事先已经非常精确地设定。这点一定要注意。

IV 鼓风机

鼓风机可以驱散催泪瓦斯或有毒烟雾。

催泪瓦斯实际上是一种细小的颗粒物 —— 您可以想象一袋面粉爆炸的那种情景，但要比这细小得多，也轻得多。当这些颗粒物落在您身上时，它就会停留在那里，以后还可以再被激活，尤其是被水或汗水激活。

出于这个原因，示威者会使用鼓风机吹掉人们身上的催泪瓦斯。

[image]

注意不要将催泪瓦斯吹向可能影响到其他人的方向。

如下面香港的这段经典视频所演示的，一个鼓风机就可以将一罐气体吹离人们，直到其他人能够将其扑灭。

https://vimeo.com/512156496?fl=pl&fe=sh

但是为了获得最佳效果，请同时使用多个鼓风机：

https://vimeo.com/512157179?fl=pl&fe=sh

当您在选择鼓风机时，要确保它有一个好的风扇和无线电源。

鼓风机与雨伞和盾牌结合使用效果很好。盾牌可以保护示威者免受冲击弹药的伤害，而鼓风机可以让有毒气体远离示威者，直到有人跑上前去将催泪瓦斯罐子熄灭，或者将罐子扔回给镇压部队的一方。团队合作很重要!

在下面这段视频的开头，您可以看到这种方法的一个例子：

https://vimeo.com/512158033?fl=pl&fe=sh

这篇文章追溯了鼓风机作为斗争工具的起源，从香港抗议到 “dad bloc” 在波特兰的首次亮相。

在波特兰冲突期间的某些情况下，手持鼓风机和其他工具的示威者能够将联邦雇佣军部署的催泪瓦斯完全控制在围栏内：

https://vimeo.com/512158919?fl=pl&fe=sh

出于相同的目的，波特兰的一些人采用了其他效果较差的工具（例如，电风扇）。

波特兰的联邦雇佣军不甘示弱，使用雾化器向示威者喷洒毒气：

[image] [image]

V 伞

伞可以同时发挥多种功能。

一把伞可以阻挡胡椒喷雾的流向。在示威活动的前面摆上一整排雨伞，可以挡住驻扎在屋顶上的监视摄像头和警察监视者的视线 —— 例如，可以掩盖防御围栏的接口，或者使更换衣服或采用其他战术更加安全。

虽然雨伞不能可靠地替代盾牌，但它也可以帮助挡住警察的榴弹、绿色和蓝色火药信号弹，以及警察用的激光侦查器。

[image]

2017年1月20日，在反特朗普的激烈抗争中，一把雨伞就发挥了关键作用，使大批 black bloc 的示威者能够冲出警察的包围圈，逃脱了逮捕。此前在香港的示威活动中，雨伞已经成为一种反法西斯主义的象征。

在波特兰，拿伞的人与拿盾牌的人并肩作战，形成一个方阵，可以在街道上保持一线，为后面的人提供掩护和保护。至少在一个案例中，示威者通过这样的队列缓慢前进，迫使联邦雇佣兵退回到他们的区域内。

雨伞、盾牌和鼓风机一起并肩作战：

https://vimeo.com/512163185?fl=pl&fe=sh

就警察而言，他们毫不犹豫地随机盗取游行示威者的雨伞。

VI 盾牌

到目前为止，在波特兰，盾牌大多用于防御来自远处的攻击 —— 比如冲击弹药、催泪弹等，而不是用来对付警棍。

[image]

不同的盾牌设计更适合不同的情况。就像雨伞和鼓风机那样，大量的盾牌聚集在一起可以做一些它们无法单独完成的事。如果您想形成一面盾墙，理想的情况下，您的盾牌应该足够大，能够覆盖您的身体。但是您的盾牌越大，就会越重，越笨拙，越难以运输。小的盾牌可以更轻，更容易潜入抗议区。

很多人除了维护盾墙之外，还一直带着小盾牌，同时扮演着其他角色。

有了哪怕一点点的保护，都能让人免于遭受重伤，也能让人有信心守住原本可能无法守住的地盘。

[image]

常见的波特兰盾牌设计是将一个塑料桶垂直切割成三个或四个弯曲的矩形，从桶的顶部和底部留下扇形底，用于制作小型盾牌。

另一方面，为了形成盾墙，最好能够将盾牌排成一排，使它们略有重叠，因为即使盾墙有轻微的断裂，也会造成漏洞。因此，在该特定应用中，胶合板可能比塑料桶更可取。

波特兰的一些人已经尝试在盾牌的边缘使用润滑剂，以使警察在进攻时更难以抓住抗议者的盾牌。

[image]

确保您在承受打击时使用了有效的技术。如果您使用的是高大的盾牌，要把盾牌非常紧地贴着身体，胸口中心的位置，这样会让您更难被移动，防止对手借助盾牌的力量把你推来推去，确保即使您的盾牌被移动了，也能覆盖您的身体。

奥克兰的盾牌墙，声援波特兰的示威者：

https://vimeo.com/512168476?fl=pl&fe=sh

缅甸抗议者对盾牌用法的演示：

https://vimeo.com/554571375?fl=pl&fe=sh

VII 体育器材

您可以用体育器材接住催泪瓦斯，然后扔回去。就像您使用鼓风机那样，确保您与其他示威者沟通良好，并有一个关于您将如何处理瓦斯罐子的深思熟虑的计划—— 这需要在策划阶段完成，即 周密的行动计划 。

最有效的工具包括长曲棍球棒、飞盘、厨房手套等，任何能让您在不直接接触瓦斯罐子的情况下把罐子扔出去的东西。

示威者也曾用曲棍球棒击回罐子。有些人一直在升级他们的雨伞 —— 例如，将雨伞倒扣在曲棍球杆或曲棍球杆手柄上，让它变成两面都可以用，必要时可以将工具翻转过来，在特定情况下使用最合理的一面。

虽然网络上有很多视频，有人试图用交通锥等物体遮盖催泪瓦斯罐，但用容器装水灭火是更好的主意。下面的视频展示了如何扑灭催泪瓦斯罐：

https://vimeo.com/512169953?fl=pl&fe=sh

VIII 气球和泡泡

[image]

示威者用气球来显示风向，以便知道催泪瓦斯会往哪个方向吹，并在背风的方向上策划一个集结点。

[image]

他们还利用泡沫来嘲笑警察的力量：

https://vimeo.com/512172300?fl=pl&fe=sh

IX 激光器

在波特兰，示威者用激光迷惑警察和联邦特工；它们还可以使监控摄像头失效。

值得注意的是，在俄勒冈州，用激光对准别人的脸是明文规定的违法行为，而且比防毒面具、盾牌和鼓风机等防卫工具更能引起警方的暴力镇压。事先了解您本地的法律很重要。

[image]

那些自己使用激光的人已经成为逮捕的目标，或被胡椒球和橡皮子弹击中，因为很容易追踪激光的来源，除非操作激光的人在两次使用激光之间迅速移动。

[image]

7月的最后一个周末，在波特兰看到的激光几乎都是比较便宜的绿色激光，303的（约50mW），可以集体部署，提供掩护，刺激警察。但更强大的蓝色的（约1w到4w）对警察、直升机和无人机更有效。

[image]

返回：https://iyouport.substack.com/p/39a?utm_source=publication-search

返回：[image]5种常用的“击落”无人机的方法

波特兰人还将激光的使用与频闪功能的大功率手电筒结合起来，以防止警察对人群的观察。使用强光灯进行逆光照射，可能会使警察难以识别出最前面的个人。

[image]
https://vimeo.com/512174837?fl=pl&fe=sh

X 涂鸦

这是显而易见的，几乎不值得一提，但示威者在发生冲突的地区到处涂写鼓舞人心的信息，突出了参与者的决心。

联邦特工为了摆出一副无助的受害者的姿态，故意不清理法院上的涂鸦，而事实上他们的暴力挑衅才是整个冲突序列的主要原因。

尽管如此，虽然联邦财产上的涂鸦图像可能会激怒那些已经支持特朗普及其走狗的极右翼选民，但这些图像也传达了那些站出来反抗当局的人的勇气。

如果您擅长涂鸦，请注意下面两件事，以尽可能避免被警方追捕：

[image]

返回：✍笔迹分析 ；✒痕量证据鉴定

XI 漆弹

示威者用漆弹来干扰戴面罩或使用透明盾牌的警员的视线。警察需要清晰的视线才能继续攻击人民。

[image]
https://vimeo.com/512177812?fl=pl&fe=sh
[image]

制作漆弹的经典模式之一是将一个小气球充气，然后反复浸入蜡中，直到蜡层能保持形状，然后放气取出气球，在蜡容器中注入油漆。其他容器，如空心的圣诞树饰品，也可以起到同样的作用。您可以在这里找到更多信息。

XII 焰火

用烟花作为投射物来迷惑或阻止警察和联邦特工的行动，无论是在当时还是在事后流传的镜头中，都有奇妙的视觉效果。通常情况下，将烟花瞄准人是不负责任的，但这里的国家雇佣兵配备了大量纳税人资助的护具，这可以说是防止他们伤害他人，而不是让他们处于危险之中。

另一方面，许多示威者都表示，由于警方部署的闪光弹榴弹的轰鸣声造成的持续创伤，烟花的轰鸣声引发了他们的创伤后应激障碍。您需要衡量利弊，任何事都要有所取舍。

XIII 火

波特兰的抗议者用火来分散警察的注意力，或者营造庆祝的氛围。这样做的时候必须要非常注意安全问题；在某些情况下，树木或人类已经暴露在火焰之下。一些抗议者使用高空烟花在远处放火。

关于在这些抗议活动中用火是否合适的问题，在注重象征性抗议的示威者和注重直接对抗的示威者之间引起了激烈的争议。镇压警察一直在迅速灭火，警告人们不要放火，并对放火者进行骚扰。

所有有关的火灾都纯粹是象征性的 —— 与明尼阿波利斯第三分局被烧形成鲜明对比的是，抗议活动中并没有任何重要的东西被烧毁。火被用来烧旗帜、垃圾、麋鹿雕像及其被拆除后的位置，有一次还烧了警察工会（PPA）大楼里的一小堆小册子之类的东西。所以所有的争论都是关于象征性的火焰。

抗议者争相扑灭象征性的小火：

https://vimeo.com/512178274?fl=pl&fe=sh

XIV 推倒围栏

自5月底以来，警方在波特兰设置了数道围栏，试图控制示威活动，示威者多次试图推倒或迁移这些围栏。早期的围栏大多是普通的铁链围栏；抗议者将一系列这样的围栏称为 “The Sacred Fence” 。

要提醒注意的是，有时，被拆掉的围栏被丢弃在街道路口，造成了绊倒或伤害的危险，尤其是当警察随后用催泪瓦斯攻击时，迫使暂时失明的示威者仓皇撤退。拆除围栏后一定要注意放在哪里，要放在安全的地方，不要给自己人的撤退制造障碍。

7月下旬，当局使用了较坚固的框架、栅栏在联邦法院周围建起了一道工业屏障，后面用混凝土块固定。在随后的夜晚，这些砖块被移到了前侧；抗议者和记者经常站在这些砖块上，但联邦雇佣兵会用冲击弹药武器对那些站在砖块上的人进行大量射击。

7月25日，一些示威者配备了电动工具，包括一台便携式角磨机，成功地推倒了一段围栏。角磨机在围栏的一角被有效地使用，但在完成工作之前就用完了电池。教训：先充电，带好备用电池。

[image]

电动工具的使用技能可能是新的；伞和盾牌对于保护抗议者免受监视摄像机和冲击弹药的伤害至关重要，而鼓风机可以防止毒雾。

正如阿基米德所说，“给我一个足够长的杠杆和一个可以放置它的支点，我就能撬动地球”。最终，这段围栏被宽大的人群向抗议者一侧拉倒，此前曾有人试图在使用角磨机的地方用一排人拉着绳子将其扳倒。

[image]

可能的改进措施包括完成切割，或用大锤敲击未完成的切割。安排两组绳索在切口的缝隙左右两边拉动可能是有意义的：两条链子而不是一条链子。正如人们在推翻雕像的过程中发现的那样，要用没有弹性的带子或链条，而不是用绳子。

抗议者曾用部分铁链围栏作为“盾牌”，但这些并不能阻挡毒气或冲击弹药。他们也曾用它们至少是象征性地“阻挡”法院大门从外面关闭。这实际上从未阻止过联邦特工，因为从来没有人试图堵住法院后面的大门。

[image]

一方面，示威者用膨胀的泡沫填充了围栏的一部分，以防止联邦特工射穿它：

[image]

撼动或推倒围栏是否可以接受，成为警察和前线人员争论的焦点：

https://vimeo.com/512182050?fl=pl&fe=sh

围栏倒下之后：

[image]

XV 解除逮捕

在波特兰的冲突中，示威者多次从企图绑架他们的警察和联邦雇佣兵手中解救人们。通常只有在示威者人数大大超过企图绑架他们的人时，才有可能成功地解除逮捕。

为了成功，行动必须发生得非常快，以至于没有时间让警察或特工的增援部队作出反应。

解除逮捕是有风险的，可能导致比最初的逮捕更高的指控。这不是一个可以轻易采用的战术。然而，如果人数和力量的平衡对示威者有利，成功的解除逮捕可以向当地政府或联邦雇佣军表明，不值得与一群抗议者搏斗，说服他们转而采取驱散战术。

XVI 群众运动

[image]

一般来说，只要警察不准备对每个人进行大规模的逮捕，当警察冲进人群将人群分开时，个人避免被逮捕的最可靠的方法是跟随人群中最大的部分。这是因为—— 在其他条件相同的情况下，最大的人群通常是最难对付的。这种见解是可以扩展的，对抗议者队伍来说，最好办法是尽可能地保持大人群。

我们已经在波特兰的人群中看到了这一点，在那里，人们已经学会了在警察进攻的时候，大群的人紧紧粘在一起，缓慢而冷静地移动，而不是奔跑，也不会比最必要的时候退缩更多 。

关于这一点，有这样的歌谣：“待在一起，紧紧地待在一起，我们每天晚上都这样做。” 提醒大家，如果能在第二天晚上和更多的朋友一起更安全地完成同样的行动，就没有理由冒着特殊的风险去保护自己的人身安全了。

当然，还有其他因素需要注意。与一个意识到周围环境、脚步敏捷、有自卫能力的团体在一起，总比与一个迟钝、混乱、容易被吓倒的团体在一起要好。您需要有选择标准，并且您的队伍需要足够的事前训练。

在波特兰，我们多次看到警察采用 “冲锋陷阵” 的方式，他们全速冲锋，同时使用催泪瓦斯、胡椒喷雾、冲击性弹药和警棍的组合来对付路过的所有人，而不仅仅是抗议者。如果您不属于足够大的人群，也没有足够装备来防止警察伤人或瞄准个人，那就要做好快快跑的准备。警察不可能冲刺很远。

XVII 阻止摄像头，破坏窗子

人们用油漆和其他手段来阻止监控摄像头拍摄示威者。

一些示威者还打碎了窗户—— 这种战术可以将警察的注意力从抗议

者真正想要做的事上吸引过去。

[image]

如果您参与任何形式的活动，穿戴得当都是尤为重要的（见上文）。在事件发生后，将您所穿的衣服全部处理掉，这可能是值得的。什么是更昂贵的？再去一次旧货店，还是保释金、诉讼费和律师费？别心疼那几件衣服。

https://vimeo.com/512185159?fl=pl&fe=sh

XVIII 法律协助，监狱协助

组织适当的法律支持是非常重要的，镇压部队每天晚上都会逮捕人。即使您不能去参加行动，您也可以帮助人们保释出狱，或者筹钱捐给保释基金。

一个结合了本文介绍的所述各种战术的运动 —— 示威者在波特兰的行动 —— 可以帮助您在面对相当多的国家暴力时保持住抗议空间。这些战术在您的国家也是重要的。

[image]
[image]

警用武器常见伤害及基本处理方法：街头实战指南 **S05E06**

[image] 关键词	团队 威胁响应 街头 街头医疗 防暴武器
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月9日
[image] **Description**	行动安全性

本文是给抗议者团队中医疗救助小组的参考资料，包括伤者应该了解的知识。不要碰您未知的领域，如果您不确定自己的行为是否得当，就去找更专业的人，避免二次伤害。

- Table of Contents

请始终优先考虑日子最新的来源，并使用基于证据的做法：
这些说明的起源
关于警用武器造成的常见伤害的非详尽说明
I. 化学制剂
A. 催泪瓦斯
i. 低浓度时
ii. 高浓度或频繁重复接触催泪瓦斯时
II. 闪光弹榴弹和其他爆炸装置
A. 爆炸伤
i. 撕裂耳膜：
ii. 内耳爆炸伤
iii. 爆炸导致的肺部损伤
iv. 爆炸导致肠道伤害
v. 切记！

B. 弹片伤
按损伤部位治疗：
i. 胸部、腹部、面部
II. 四肢
i. 大的伤口大的异物
ii. 看起来是良性的小穿刺伤口，但深度不明
III. 橡皮子弹伤害
A. 按伤处划分
i. 四肢大面积瘀伤
ii. 面部伤
iii. 眼睛伤
iv. 鼻部撞击
v. 胸部撞击
vi. 腹部撞击伤
vii. 腹腔和胸腔冲击伤
viii. 下背部撞击伤
ix. 睾丸伤

[image]

以下准则旨在使街头医务人员和医疗救助队员能够应对警察暴力造成的一些常见的伤害。

这些准则是根据法国政府试图在圣母院建造机场但最终失败了的反抗斗争中收集的经验制定的。如果根据现实生活中的经验，很难找到关于如何治疗这种伤害的可靠信息。

请注意，大多数主流的医疗专业人员在治疗 *警用武器造成的伤害* 方面经验都不够；本指南分享了医护人员在反复应对这些伤害时获得的知识，希望能让其他人免去试错学习的麻烦。

正如“不伤害联盟”（Do No Harm Coalition）曾经优雅地指出的那样，受过医学训练并不意味着你有资格成为一名街头医生。街头医务人员在不断发展的讨论中、从分享关于什么有效和什么无效的信息中获益。

这里列出的危险信号也可以帮助受伤的人识别自己的症状何时严重，何时应该寻求专业的医疗护理。

这些指南并非详尽无遗，可能有许多事没有包括在这里。例如，在2018年4月和5月期间，警方对 ZAD 抗议者部署了数千枚催泪弹和闪光弹榴弹，但胡椒喷雾相对较少。本文将基于最常见的镇压武器加以分析。

下面的内容不是一个自己动手的指南。您所在的地区或附近的大城市很可能有一个街头医疗队，您需要首先找到他们！如果真的没有，那就组建一支自己的队伍，调用那些有外科基础知识的人，但他们不一定擅长治疗警用武器造成的伤害；在他们的基础知识之上得到更专业的培训。

医疗队有时也会对新加入的医疗人员进行自己的培训。这里详述的许多做法需要广泛的知识和经验 —— 如果做错了，真的会伤到人。您要小心。请不要通过声称您没有的经验或试图在您的知识范围之外鲁莽尝试来危害他人的健康。

[image] 照片来自于 Ujimaa Medics，这是一支由黑人女性在芝加哥成立的救助小组，他们培训社区应对城市紧急情况的第一反应。

以下是一些资源，可以帮助您获得更多关于街头医生的历史和实践的信息 —— 从它作为民权运动期间的自卫工具开始，到它在最近发生的抗议中的使用。

请始终优先考虑日子最新的来源，并使用基于证据的做法：

- 现代街头医务人员简史
- 街头医生：保持我们的反抗运动健康和安全
- 在哪里可以找到你当地的医疗团体—— 这个信息并不总是最新的，但提供了一个很好的起点
- Rosehip Medics—— 是一个历史悠久的医疗团体，在他们的网

站上提供了各种信息，从“反叛和大流行病中的健康和安全”到关于紧急医疗服务替代品的免费小册子

- Paper Revolution—— 解释了成为街头医生的一些方法，并提供了更详细的实用信息的链接，如他们的街头医生指南或暴动医学指南

下面是近期医护人员联盟进行培训的视频，内容涉及如何在街道上保持安全和健康：

[image] 下载

这些说明的起源

下面的说明是由ZAD治疗师小组编写的，这是一个跨学科的团队，由护士、医生、街头医生、药师、心理学家、自然疗法医师和积极人士组成，他们是参与保卫圣母院ZAD（Zone à Défendre）斗争的医疗工作者大网络的一部分。

用他们的话说就是：

> 在2012年秋季的驱逐行动中，一些医疗专业人员来到现场支持医护人员。多年来，我们一起准备后勤和通信战略，并保证在发生驱逐企图或其他警察干预的情况下拥有必要的设备。我们还定期进行讨论，并定期进行对等的培训。
>
> 一旦反抗者将异议转化为具体的行动，或者阻挠企业型经济的顺利运转，镇压就会迅速跟进。不管是抗议的时间长短，还是因为我们住错了街区，或者因为我们的肤色，当我们被贴上“不受欢迎”或“暴徒”的标签时，国家就会通过执法部门对我们进行伤害和杀戮。
>
> 意识到这些风险，许多国家的革命团体和激进运动组

织为示威或直接行动发展了自己的医疗支持网络。这种做法与红十字会等人道主义团体完全不同，因为我们不会假装中立。我们采取明确的政治立场，并在冲突中和在我们对同道的支持中发挥积极作用。

在一次示威活动中，街头医疗队都试图尽早赶到现场，以便能够为要求急救的人提供紧急护理，并在救护车到达之前评估情况的需要，而救护车有时会被警方阻拦或拖延。此外，还对求助于官方急救服务所涉及的法律风险进行了评估：例如，在医院内对无证件者、有未执行逮捕令者、或仅仅因为受伤的事实使某人成为嫌疑人而遭受身份检查甚至被直接逮捕的风险。

警方会定期更新他们专门用于镇压的设备，配备新的化学、电子和物理武器。作为街头医务人员，我们试图通过传播在当地开发的防卫技术来应对，并在世界各地分享预防、保护和治疗的知识。

对我们来说，医学知识伴随着政治反思，我们如何将其付诸实践，以避免重现普通医疗机构所特有的统治、管理和剥削关系。作为街头医务人员，我们希望优先征得伤者的同意，并向他们提供所需的信息，以便他们能为自己做出明确的和知情的选择。

……

—— 以上内容摘自2015年ZAD街头医务人员的声明。（以印刷形式出版；不可在线获得）

[image] 一枚催泪瓦斯榴弹

关于警用武器造成的常见伤害的非详尽说明

以下说明是在2018年一次驱逐ZAD之后编写的，在此期间，由于警察用坦克阻挡救护车，医务人员建立了一个平行的紧急护理系统。

这些说明以获得特定资源和技能及知识为基础；为了清晰化和背景化，它们已被编辑。

这些说明中的许多都假定有能力获得医疗护理和转移到医院作为备用选项。如果您的国家没有全民医疗，如果您自己也没有医疗保险，但与您社区中的医疗工作者有联系，请向他们索取资源，或与您周围的人合作，寻找其他方法获得您所需的护理。

这些指南是为训练有素的街头医务人员和医疗工作者应对警察暴力而编写的。它们不能代替正规医院的医疗或诊断。请不要在您的专业范围外执业!

I. 化学制剂

催泪瓦斯又称CS、CN或CR气体，是一种气溶胶，对呼吸系统有刺激作用。胡椒喷雾剂是一种含有辣椒素的红色油性物质，从辣椒中提取，直接喷到皮肤和眼睛上，形成强烈的刺激。

[image]

A. 催泪瓦斯

i. 低浓度时

—— 症状：皮肤和眼睛感觉刺激和烧伤。

—— 处理方法：尽量用水压冲洗或轻柔摩擦冲洗。

眼睛：用生理盐水溶液冲洗（水+盐，每升9克）。它不需要是无菌

的。

皮肤：用90%的水，10%的美乐事 Maalox，或者水加4%的小苏打混合。如果您没有这些东西，普通的水就可以用来治疗 *低浓度* 的催泪瓦斯。

注：催泪瓦斯会导致呼吸困难或引发哮喘发作。对于有哮喘病的人来说，如果他们感觉喘不过气来，可以采用沙丁胺醇，甚至口服强的松（由有经验的医生指导）。之后几天内避免接触催泪瓦斯。

注：Maalox 是赛诺菲（Sanofi）拥有的抗酸剂品牌。他们的主要产品是含有氢氧化铝和氢氧化镁的调味液，其作用是中和或减少胃性物质；沙丁胺醇，常见商品名泛得林，为一种用于扩张肺部大型及中型气管的药物。可用于治疗气喘相关病症，例如气喘急性发作、运动诱发性支气管收缩，以及慢性阻塞性肺病。沙丁胺醇常配合定量吸入器或雾化器使用，但亦可制成药锭或静脉注射。吸入剂型约15分钟内即可见效，效用可持续2至6小时。

ii. 高浓度或频繁重复接触催泪瓦斯时

—— 可导致残疾或其他神经系统症状：恶心、呕吐、剧烈头痛、精神错乱。在这些表现中：

- 排除脑震荡！
- 了解损伤的机制。发生了什么？毒气？榴弹爆炸的巨响？撞击了头部？高处坠落？…… 询问伤者和目击者关于具体情况。
- 伤者是失去了知觉还是能记得一切？

对于疼痛: 布洛芬

对于中度恶心和呕吐：口服或栓剂类抗恶心药物，如甲氧氯普胺；姜

片和薄荷或甘菊茶也能有帮助。

对于严重的呕吐和无法喝下任何液体或药物（有脱水的风险）：转到医院进行静脉输液和观察。

对于严重的丧失意识：不要口服药物，将伤者置于恢复位置，并呼叫救护车。

注：确保人们知道在拿起或接触催泪瓦斯罐之前要戴上厚的皮手套或专门的耐热手套（如烧烤手套），以避免烫伤。

注：甲氧氯普胺适用于治疗胃及食道问题的药物。本品主要用于治疗恶心和呕吐，并可协助胃排空障碍的患者排空胃部，并治疗胃食道逆流。

[image] 闪光榴弹爆炸的情景，近距离爆炸容易导致人失去意识

II. 闪光弹榴弹和其他爆炸装置

A. 爆炸伤

爆炸伤主要损伤耳朵。

i. 撕裂耳膜：

- 根据我们的经验，这种情况不常发生。不是紧急情况。
- 症状：疼痛，耳朵出血，听力暂时下降。
- 治疗方法：用耳镜检查耳朵，最好在24小时内完成。耳膜撕裂的情况会在2周内自愈。

- 如果可以进行体检，可以预防性地给予8天的抗生素滴剂（氧氟沙星滴剂），以避免中耳和邻近区域（鼓膜后）的感染。在任何情况下，10至15天后到初级保健部门复诊是最理想的，以便进行耳镜检查，如果有持续的异常，则转诊到耳鼻喉专科。

ii. 内耳爆炸伤

- 根据我们的经验，这种情况经常发生！

- 症状：疼痛、耳鸣、听力下降、眩晕或头疼。

- 耳鸣不是来自于鼓膜，而是来自于内耳。听力损失程度是治疗的指导因素（而不是耳鸣）。

- 简单的听力测试：用拇指与其他手指在人的耳朵旁边摩擦。问他们是否能听到，然后在另一边做同样的事。

- 治疗方法：如果在爆炸后24小时内仍有听力损失现象，请尽快与耳鼻喉科专家预约。为了避免或至少限制永久性的听力损伤（由于内耳细胞死亡造成的），可能需要使用类固醇：耳内注射泼尼松龙（0.5mg，1mg/kg/天，持续2–3天）是最常见的处方。

iii. 爆炸导致的肺部损伤

- 根据我们的经验，较少发生。

- 症状： 事故后几天内出现呼吸困难。

- 治疗： 急诊。肺水肿需要住院治疗。当气泡从肺部进入血液并进入大脑时，由肺部爆炸伤害引起的空气栓塞可导致癫痫、中风和/或永久性脑损伤。

iv. 爆炸导致肠道伤害

- 根据我们的经验，较少发生。

- 症状：在爆炸后的几天内出现腹痛、便血，可能表明肠穿孔。发热和腹胀（胃部发硬）可能表示腹膜炎。

- 治疗： 这两种情况都是医疗紧急情况，需要住院治疗！

v. 切记！

- 使人远离额外的噪音。

- 如果伤害对认知功能有影响、或对器官有损害，请毫不犹豫地联系紧急医疗提供者。

- 建议在24至48小时内就耳部爆炸伤害进行ENT专家会诊，一定不要延误！时间很重要。如果您不想造成永久性伤残的话。

- 观察爆炸伤患者数天。表明并发症的症状可能会延迟出现，如听力、呼吸、和腹部功能的变化。

B. 弹片伤

根据我们的经验，弹片伤经常发生。弹片往往是塑料的，有时是金属的。闪光弹榴弹在撞击人行道时，可将泥土和沥青与弹片一起推进；这就增加了感染的风险。有时入口处的伤口很小，甚至几乎很难看清楚；有时则是非常大而明显的。

请注意，弹片伤是严重的，即使它们起初看起来不是什么大事。检查、观察和跟踪都至关重要的。

永远不要接近或捡起一个还没有开始冒烟的罐子。它可能是一枚闪光弹榴弹，严重的情况下会炸掉你的手。这在ZAD和 Gilets Jaunes 的抗议活动中都发生过。

先检查和评估伤口的宽度和深度，然后再包扎。

按损伤部位治疗：

i. 胸部、腹部、 面部

紧急情况：有潜在的生命危险。要看有经验的医生。疏散并评估呼吸/神经/心血管系统的不适和出血的程度。

II. 四肢

检查一下：

——关节受损。

——神经损伤。

神经损伤需要立即住院治疗！ 检查伤口上下的脉搏、运动、感觉，比较一下旁边的肢体，作为参考。看是否有麻痹、虚弱或活动范围困难。麻木、刺痛或针刺感表示神经损伤。

——肌腱受损：

- 尤其是手和脚。
- 常发生于手背处的伤口（有指甲的那一边）。

- 症状/体征：伤口底部有明显的肌腱损伤，或根据解剖学怀疑有肌腱损伤。

- 活动范围正常并不代表肌腱没有损伤。

- 治疗方法：如果怀疑是肌腱损伤，请去看有经验的医生。可能需要在24小时内进行手术干预，以避免破裂的风险。

根据弹片的大小来清除弹片。所有大块的弹片都必须取出。

i. 大的伤口大的异物

——不经常发生

——治疗：请找有经验的医生，将病人转诊到医院或取出异物并缝合皮肤，运用优秀的解剖学知识，通过后续护理和预防性抗生素控制感染风险。

ii. 看起来是良性的小穿刺伤口，但深度不明

——经常发生。

——治疗：清洁、包扎、跟进；如果有许多明显的浅层异物 (如从滑板上摔下来那种严重擦伤)，蜂蜜敷料可将其引出，而无需物理清除。密切观察是否有感染。

局部治疗：

- 直接按压可以在大部分时间内止血；

- 每个开放性伤口都需要基本的卫生处理! 医护人员必须用肥皂和

水洗手，并戴上医用手套，在处理每一个伤员之前都要换手套。

- 尽快用 Betadine 肥皂 (红色的那种) 擦洗：一些被弹片刺伤的伤口并不能立即看到。

清洁和干燥：

用肥皂和水清洗伤口（如果没有肥皂和水，则用无菌盐水清洗）。

接着用双氧水，它有发泡的优点，有时可以抽出小块弹片。

如果异物很小或很难看清，用无菌镊子，但不要撕扯它或使状况变得更糟! 身体会自然地拒绝小碎片，或者在它们周围形成一个缓冲区。当弹片进入身体时，伤害已经完成；额外的风险是感染。

注：

- 使用无菌医用镊子。普通的镊子（用于去除毛那种）太大，会撕裂皮肉。

- 磁铁可以帮助清除金属弹片。将弹片从进入的路径拉出来——要小心！否则，你可能会制造一个新的伤口。

- 如果太痛，可在伤口底部使用利多卡因喷雾等局部麻醉。

用消毒剂消毒：

- 记住：如果消毒剂的瓶子开封超过一个月，就不能要了。开瓶后在瓶子上标明日期。优先使用小瓶，避免过期。

- 黄色的 Betadine、聚维酮碘。(如果无法用肥皂和水清洗的话，

先用红色的Betadine)。碘过敏者不适用于**Betadine**。

- 氯己定是好的，比如一次性使用的 Dosiseptine，但不要用比塞普汀（酒精类的），因为它会刺痛。

- 稀释的次氯酸盐（Dakin’s solution）效果很好，但必须用无菌水稀释50%，所以不实用。酒精是有效的，但烧得很厉害。

- 用于穿刺伤口：消毒表面和内部，使用不带针头的消毒注射器。注射前将注射器的末端放在伤口内。不要使用双氧水。

注：聚维酮碘，又称优碘是用于手术前后皮肤消毒的杀菌剂。其溶液是中国大陆称碘伏的一种。它可以用于消毒患者的皮肤和医护人员的手，用于轻微的伤口，能以液体或粉末的方式应用于皮肤上。氯己定为外用抗菌剂及阳离子表面活性剂，对多数革兰氏阳性菌和革兰氏阴性菌具杀灭作用。除可抑菌外，也可杀灭一般细菌。

包扎：

– 近似于控制出血的伤口：干绷带、纱布敷料、弹性绷带。

– 伤口渗血或化脓：可以考虑用吸收性的垫子，比如止血包扎，然后在上面加压和绷带包扎。

– 如果是中度出血或未愈合的伤口：用干净的生蜂蜜（不是玉米糖浆的那种）、新孢霉素或敷伤巾，然后敷料和绷带。

注：敷伤巾 tulle gras 敷料是法国常用的一种绷带，它由浸有软石蜡油，秘鲁香脂和橄榄油的织物组成，可防止其粘在伤口上，但意味着它需要与另一种吸收性敷料结合使用。

更换敷料：

– 开始时每24小时更换一次 (视严重程度而定)，然后每48小时更换一次。

– 用生理盐水溶液冲洗。不要再涂抹消毒剂，因为这样会延迟愈合。

– 防止二次感染。弹片伤经常会出现这种情况! 感染的迹象包括发红、发炎、流脓、流泪或发烧。在受伤后48小时内，请找有经验的医生咨询，并服用或局部注射抗生素。

– 脓肿可能需要进行X射线检查、超声波检查或手术咨询，这取决于伤口的情况。

受伤的人请注意：如果您出现发烧、发冷、僵硬、发红、伤口周围湿润、皮肤上出现红色斑块或条纹，或出现神经系统或运动障碍，请咨询医生、或立即去急诊室。

弹片伤心得：

不要太用力挖出小碎片。

立即评估是否有神经或肌腱损伤。

监测是否有继发感染的迹象，并持续数天。

III. 橡皮子弹伤害

橡皮子弹伤往往会留下很大的瘀伤。要检查是否有其他病变! 如果您怀疑是需要手术的外伤，不要给伤者吃任何东西。不能喝酒，不能吃东西，不能抽烟。

[image] 橡皮子弹

A. 按伤处划分

i. 四肢大面积瘀伤

– 评估神经血管状态：脉搏、运动、感觉和颜色。如果有异常，急需住院治疗。

– 摸摸骨头，看看有没有针刺式的疼痛和蠕动。测试每个关节的活动范围。如果不能排除骨折的可能，24小时内要去做X光检查。如怀疑有移位骨折，需要立即拍X光片。

– 橡皮子弹对肌肉和肌腱的撞击不属于紧急情况。

– 用山金车（Arnica montana）酊剂或凝胶或地雏菊（Bellis perennis）酊剂治疗所有瘀伤或血肿，尽快局部使用（实际的酊剂，不是顺势疗法）。

– 如果计划住院，在应用外用治疗之前要等待：因为它可能会掩盖病情的严重性。

– 最重要的是固定受伤部位。

ii. 面部伤

– 看有经验的医生。

– 触诊面部骨骼，寻找表明骨折的针尖状疼痛和蠕动：眼眶、鼻子、颧骨、下颌骨、下巴、牙齿衔接状况（闭合和对齐）。检查每颗牙齿。

– 对于断裂、移动、不固定或疼痛的牙齿 —— 立即看牙医。用牛

奶、盐水溶液或唾液保存掉落的牙齿。理想情况下，伤者会把它含在嘴里，注意不要吞咽。

简单的神经面部评估：

- 轻触，比较额头、脸颊、下巴两侧的感觉。
- 动作：微笑时对称，紧闭时双眼对称，眼球运动（双向、垂直、水平、对角等），瞳孔等大、圆润，对光反应灵敏。

iii. 眼睛伤

– 立即住院治疗。

– 不能吃东西，不能喝水，不能吸烟。

– 用无菌盐水溶液冲洗局部。

– 让患者躺下，用无菌敷料覆盖双眼。

iv. 鼻部撞击

– 可能是骨折

– 做个X光检查

- 鼻衄是指鼻子出血，不要小视，它可能会变成大出血。

处理：

- 用两根手指捏住鼻梁，脖子向前弯曲
- 有经验的医护人员可以用纱布堵住鼻孔
- 如果失血量大，要叫救护车

v. 胸部撞击

– 疼痛可能表示肋骨骨折或肺部受损。请看有经验的医生。

– 肋骨骨折：沿胸骨线触诊时有针刺痛感。

- 深吸气时疼痛。
- 没有呼吸困难或咳嗽。
- 如果是单纯的骨折，用休息、止痛药治疗，保证深呼吸，避免肺炎，局部用紫草药膏（Symphytum officinale），每天2～3次。

– 气胸：疼痛和咳嗽，有时吐血。

- 24小时内拍X光片，如有呼吸困难则立即拍片。
- 监测呼吸频率。正常为每分钟15–20次呼吸。

vi. 腹部撞击伤

– 要看有经验的医生。

– 检查：

- 肝脏 (右上腹) 和脾脏 (左上腹) 周围的疼痛: 内出血的迹象表明有危险。
- 迅速做B超检查。
- 大便带血、腹痛、胃区发硬或发热，怀疑有腹膜炎：立即住院治疗。

vii. 腹腔和胸腔冲击伤

– 检查是否有内出血（休克）的迹象，如 脸色苍白、虚弱、出汗、心动过速，但血压正常。

– 晚期症状包括低血压、精神状态改变、意识丧失。

– 要观察伤者数个小时!

viii. 下背部撞击伤

– 寻找尿液中的血液。最好做个尿检，检查一下肾脏是否受损。

ix. 睾丸伤

– 如果出现瘀伤或过度疼痛，请做紧急超声波检查。

[image]
[image]

充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

[image] 关键词	心理战 移动设备 街头 逮捕 防御 预防性
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训 ；[image]被捕支援 ；[image]突袭应对措施 ；[image]数字技术限制和最佳实践 ；[image]镇压应对措施
[image] 创建时间	2025年1月10日
[image] **Description**	行动安全性

永远记得，即使在被捕的情况下，我们仍然可以继续反抗。

- Table of Contents

  1. 如果您拿定主意破釜沉舟，那就必须非常快速地行动
  2. 利用团队的中间环节，让自己得以摆脱敏感物品
  3. 不要给警察找方便
  4. 新情况＝新机会
  5. 不要带自己的手机
  6. 抓住机遇，传播技能
  7. 互相关爱
  8. 不要 和警察说话
  9. 不要相信 警察说的任何话
  10. 保持士气 (我们需要新的歌谱)
  11. 一分预防胜过十分治疗
  12. 重申：最好任何时候都不要和警察说话

[image]

2017年1月20日，美国发生了历史上最激烈的抵抗总统就职典礼的抗议事件。当天，有远超100名示威者在12号和L号交叉路口被警察包围并被逮捕。这是自15年前的人民大罢工以来，华盛顿最大规模的大规模逮捕行动，而2020年的就职典礼示威活动中的具体统计数字还没有出来。

这次逮捕使用的是水壶战术，我们曾经介绍过这种抓捕方式见https://iyouport.substack.com/p/38。在下面看到当时的场景视频—— 注意在警察的围捕“水壶”开始形成的最初，一些抗议者很有组织地号召人们冲锋，举着雨伞地抵挡警方的反击。最终只有这些人逃脱了，后面没有跟上来的100人都被捕了：

https://vimeo.com/200490022?fl=pl&fe=sh

这批抗议者与经历过大规模逮捕的前辈之间的差距显而易见。有些人无意中让警察收集到了有关他们的情报；许多人对逮捕过程的基本知识很是缺乏。

当下正是群众抗争和大规模逮捕的新阶段，本集将尝试梳理一些历史事件中的经验教训，以便帮助未来的行动者尽可能避免被逮捕、利用被逮捕、尤其是在拘留所里保护自己。

1. 如果您拿定主意破釜沉舟，那就必须非常快速地行动

周五的水壶围困中，有些人确实逃过了逮捕这一劫。一场勇敢冲锋让一些反抗者挣脱了束缚（如上面的视频），并在当天余下的时间里在街头继续战斗。

他们成功的关键是，他们冲锋的时候，最大部队的警察力量还守在12号和L号路交叉口。

[image]

被水壶围困的时间越长，就越难突围：警察会快速建立起自己的势力

和监控，被围困的抗议者会迅速降低士气。所以，如果您想尽可能摆脱这种围困逮捕，最好的机会就是在水壶战术开始实施的最初突破防线。

2. 利用团队的中间环节，让自己得以摆脱敏感物品

一旦确定被包围，你就没有逃跑的机会了，这时候你就应该立即更换服装；尽量在不被拍到的情况下更换服装。

在任何一个行动组织中，穿一套最普通的衣服在里层，都是很重要的—— 因为只有这样你才可以迅速转变自己的面貌。

在遭遇大规模逮捕的情况下，最稳妥的方法是移动到人群中心位置，隐藏在人群中看不到你的地方，脱掉任何可疑的物品—— 比如行动标识、与这场行动相关的装束等，换上你的便装，然后移动到人群的外围，为那些还没有换服装的人提供掩护。

也就是说换衣服需要有组织地交替进行，不能是一下子所有人都想要获得换衣服的机会，那将没有任何人能拥有这个机会。必须有足够多的人愿意为同伴做掩护。

在换衣服的时候，要认识到可能会让你暴露的所有细节，比如你的鞋子或背包。例如，你可以把早前背着的包包放在另一个更大的包包里面，或者放在你的黑色装备下面（外面套一个外套），或者用黑色胶带遮住鞋子上的可识别性标志。

3. 不要给警察找方便

当被扣留在12号和L号路口的抗议者人群被要求把手举起来时，大多数人都举起了手。这不是他们唯一能做的事。

[image]

请记住，我们在囚禁中能找到的安全感永远不会来自于服从命令，而是来自于我们如何利用警方要求的任何合作，而这些合作仍在我们的控制之下。

如果他们让你做什么，可能是因为这能让他们的工作更轻松。理想的情况是，被拘留的人群应该建立一个程序，共同决定如何回应警察的命令。

“非暴力直接行动”的标准指南建议建立一个警察联络系统，但在某些情况下，这可能是困难的。在2002年人民大罢工的一次大规模逮捕中，被拘留者立即被绑住了手臂，直到警察告诉人群他们会允许人们举手离开水壶。

而一起协调性不服从的行动经验能够在参与者之间建立士气和融洽的关系，这在整个余下的被关押过程中都会很有用。在J20上，警察所要做的就是在人群中穿行，指着人们让他们心甘情愿地走进一辆车。有些人只是因为无聊而自愿被捕，误以为这样可以加快释放速度。

反全球化运动经历了很多次大规模的抓捕，有很多有创意的轶事可以借鉴。

[image]

一代人之前，被捕者拒绝透露姓名，一进拘留所就换衣服；干脆在拘留所里脱光衣服，一丝不挂；在监狱里唱歌；互相锁住手臂，形成被捕者的 “人链” ，阻碍警察的任务。这些声援和反抗的事例，很多都以警察对被捕者施暴而告终，但是，有时也迫使当局释放了一批批 “John Does” 和 “Jane Does” （有趣的化名），而没有起诉。

老实说，在任何情况下我们都无法准确计算出什么样的不服从对被捕者最有利，大多数人都不想为了象征性的反抗而被打碎肋条—— 但我们不应该忘记，即使在被捕的情况下，我们仍然可以继续反抗。

□

延伸：https://iyouport.substack.com/p/30?utm_source=publication-search

4. 新情况＝新机会

在第12街和L街，一些抗议者利用了15年来华盛顿最大规模的逮捕，组织一些被拘留者发表反独裁宣言。流传的另一个想法是绝食，以呼吁人们关注 Standing Rock 的 “No DAPL” 斗争。其中许多人反正30多个小时没吃东西。

当天全世界的目光都集中在华盛顿，大规模逮捕的严重性提供了另一个机会来澄清抗议者的信息并加强其影响。

后来，在一间拘留室里，四十多名被捕的抗议者正无聊而焦虑地躺在那里，有一个人提议大家举行一次讨论，讨论我们如何能从这次经历中汲取更多的力量。

这立即改变了一群抗议者在拘留室里的基调：人们从一个个孤立的、害怕的个体，凝聚成了一股勇敢的集体力量。

5. 不要带自己的手机

虽然发生在12号和L号大街的大规模逮捕与十年前的大规模逮捕相似，但有一点是新的：警方没收了大多数人的手机。当天携带个人手机的被捕者的所有关联人、对话和社交媒体账号，现在可能连传票都不需要，就能被当局获得。

[image]

在这一点上，你不知道他们会如何使用从所有手机中收集到的信息来对付你，但这件事必须再次提醒参加行动的人们，一定要注意手机问题。

[image]

返回：[image]当您准备参加抗议活动：基本指南

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

请不要把您的个人手机带到抗议活动现场；更不要在街上拍照！——您拍摄的东西都很可能会帮助警察识别您在哪里、您周围有谁，也给警察提供调查和起诉您的队友的照片证据。

[image]

返回：[image]社交媒体上的行动主义安全性:框架手册

返回：[image]在将抗议现场的照片和视频发布到社交媒体上之前，请执行此操作

一次性手机有很多。如果你想要一部没有实名的手机，这是一个不错的选择 —— 例如，这样你仍然可以与为援助组织的短信提醒和法律热线保持同步。这里是一些选择手机的方法：

[image]

返回：[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

返回：[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

如果你被逮捕，请尽量快速销毁、抛弃或隐藏你的**SIM**卡，这样警察就无法获取你的所有信息。有律师提出，一旦手机被警方掌握，远程

擦拭手机可以算作是“篡改证据”，你会因此被起诉。即使取出SIM卡后，你的手机上可能还残留着很多东西。怎么强调这一点都不为过：不要带着您的私人手机去参加有高逮捕风险的行动。

[image]

返回 - 直接行动激进派人士请从这里进入：[image]被捕支援

以及：[image]数字技术限制和最佳实践 ；[image]突袭应对措施

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image]

6. 抓住机遇，传播技能

一旦被包围，就不能保证你们有多少时间在一起。当时一些抗议者在12号和L号大街上呆了8个小时，但如果警察有更好的准备，他们就可能会立即把抗议者拖走。

[image]

在您还有机会的时候，把本站讲述的这些技能传授给经验不足的人是非常重要的。当你们还在一起的时候，让每个人都站在同一阵线上，意味着每个人都会得到同样的信息 —— 这比寄希望于在所有运送被捕者的车辆上进行同样的对话，更有意义。

如果你是一个有丰富经验的运动老手，不要太羞于通过说话来暴露自己 —— 有你在身边，就不能让那些对基本安全文化一无所知的人犯容易预防的错误。

你也许会担心警察把你视为“潜在的领导者”而不敢说话，但是要知道，只要有一个人犯了愚蠢的错误，就会让所有人陷入危险之中，这比警察如何判断领导者更要危险得多。大家都站在同一条战线上的感觉，会让人们以后在警方的压力下有恃无恐地闭上嘴巴。

7. 互相关爱

12号大街被围在水壶里的人们有一件事做得很好，那就是互相照顾。

医护人员为人们治疗胡椒喷雾的伤害、帮助哮喘发作的人、治疗创伤后应激障碍、以及警察向被困人群发射的闪光榴弹所造成的伤害；全国律师协会的律师帮助解释了逮捕和可能的监禁程序，帮助人群中经验较少的示威者获得相关知识。一些抗议者在水壶里呆了近8个小时，所以当有人无法再坚持下去时，其他人用自己的身体和横幅遮挡，给需要如厕的人提供隐私。

当然，这里还有改进的空间。当国家分配的性别二元制通过监狱引入后，人们不加批判地就将这种二元制内化了，而没有考虑到我们的队伍里那些生活中违背出生时分配的性别中的人。

包容是反抗者队伍必需注重的事情之一，因为你们反抗的这个现实世界是不包容的，同道们都会期待在自己构建的小世界中获得更多珍贵的价值。

[image]

在任何大规模逮捕的情况下，寻找那些看起来孤立无援的人并向他们提供支持绝对是可贵的；这可以减少任何队友屈服于威逼利诱而与警察合作的可能性。

焦虑可能是反抗者最大的敌人；承认它，但不要让它统治你，并尽你所能让别人安心。

当一个人可以获得一种资源（比如一个电话、一次律师访问）时，向周围的人询问一下，看看这些信息是否能对其他人有什么好处。

在[image]直接行动分步指南：它是什么、它有什么用、如何获得成功 中我们强调过：不论如何不能出卖自己的队友。审讯者会使用各种

手段逼迫你和他们合作，从暴打到心理诱导，有些人身体很强壮，也许能扛得住暴打，但是有可能扛不住心理诱导 —— 尤其是像中国这样的互信度很低的社会里，日常情况下几乎所有人都是孤立的，长期缺乏理解、信赖和同情，当审讯者施加伪造的理解和同情时，很多人会难以抗住。避免这种情况下发生的唯一办法就是，您的队伍中必需用爱包围起来，用互爱连接所有人，不能让任何队友被边缘。只有熟悉被爱的人才能准确及时地识别审讯者制造的虚假善意。

[image]

请从本站 “ 心理安全 ” 专题查找审讯心理学的知识和防御建议。

[image]

返回：[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

8. 不要 和警察说话

必需不断重复这点 —— 您对警察说什么都不会有任何帮助，请切记！ 您只需要说：“对不起，警官，我的律师告诉我，我不应该告诉警察任何事，除了我的名字之外”。就这么简单。

一旦进了监狱，警察就会竭尽全力让你开口。其手段范围从比较无辜的样子，比如 “那接下来发生了什么事？” 到更明显的陷阱，比如 “你知道你犯的是啥罪名吧，害怕吧，现在还有机会咱可以谈谈，只要你张嘴 ……”。

[image]

即使你确定自己没有做任何违法的事，你所说的话也会让其他人陷入危险之中 —— 警察越是把你看成是一个愿意和他们交谈的人，他们就会给你更大的压力。看似不相关的谈话，都可以用来确定被拘留者之间的关联，以及以后用来对付你。

请专注于度过难关，直到你被释放。之后，在律师的指导下，你将有

足够的时间减压。

请记住，你很可能在牢房里被录音和/或录像。在拘留室内，由于身边似乎 “没有警察“，许多被捕者会感觉下意识地放松，开始公开谈论自己的生活、自己的组织工作、当天的事件以及许多其他话题，但却忘了很可能有隐藏的监视器存在。这些话题即使不直接入罪，也会给你的对手提供有关你们的行动项目和相互联系的信息，这只会伤害我们。

警察和管教人员很可能会有不公正的行为。他们是想激怒你。你可能会发现自己想告诉他们到底应该去哪里，以及其他与他们相似的卑鄙人物。还是省省吧。如果你自己憋不住，就想想其他和你一起被捕的人，为他们憋着。与警察的任何一种互动都不能改善你的案子或你周围人的案子。

9. 不要相信 警察说的任何话

一旦被捕，你就处于一种不确定的状态，在这种状态下，你对自己的处境几乎没有控制权 —— 这种不确定性可能导致的焦虑心理就是警察对付你的主要武器之一。如果你能在被拘留期间努力保证自己暂时不对潜在的结果做出情绪反应，你就能夺走警察对付你的大部分权力。

警察是很会欺负人的。他们会说谎话只是为了吓唬你：说你会面临几年的牢狱之灾，说你在监狱里会被殴打，说其他被捕者跟他们说过 “你做了什么” 。不要相信任何一个字，一切都是假的。你的案子的证据以后会很清楚，不要听信警察说的任何话。在你被逮捕的时候，要集中精力确保警察从你那里得到的信息尽可能地少，这非常重要！

即使你莫名其妙地遇到了一个真心实意的“好警察”，他们也无论如何不能做出任何决定或承诺。他们可能对实际发生的事知之甚少。他们不发号施令，他们只是向上面传递信息。

[image]

所有人要齐心协力熬过被逮捕关押的过程，而不是去纠结警察的话，那没有任何意义。

10. 保持士气 (我们需要新的歌谱)

自从被水壶围困之后，一些被捕者都抱怨过那些行动中使用的歌曲。大部分只是类似 “永远团结” 的合唱。这些歌曲在某些情况下是不错的，但这一次人们见证了华盛顿特区15年来最大规模的逮捕，而这些歌曲与十年前大规模逮捕时人们所唱的歌曲简直一模一样。

我们需要新的歌曲，让人感到新鲜和现代。当然，要找到一首大家都喜欢的歌曲是不可能的，但至少可以通过扩大选择范围来保持它的趣味性。集体歌集应该包括针对各种情绪和环境的赞歌：欢欣鼓舞的曲目，没错，但也包括凝聚力量、严肃的团结、嘲笑警察，以及在不确定的情况下传播决心的力量。

[image]

人们还需要其他方式来维持士气，同时一起打发时间，比如做游戏、讲故事和说笑话。

抗议者特别感谢所有在集会对面围观的人们，他们通过挥手和大喊声援来保持抗议者的精神状态 —— 但到目前为止，最令人振奋的支持是两个街区外的燃烧的豪华轿车从第13街传来的烟雾和橡胶轮胎燃烧的气味。这些勇气的传染，街道上其他地方的激烈抵抗声比任何歌曲都要更加甜美。

11. 一分预防胜过十分治疗

所有这些建议只要稍加预想就会更加有效。例如，如果事先稍作计划，也许被拘留者的发言就会更有说服力；上述绝食的提议也是如此。在您的亲密团队中提前计划好一旦被围困，你们会怎么做 —— 是否要突围，如何迅速摆脱可能被定罪的一切物品，谁会携带一次性电话，以及如何处理它们。

[image]

更多内容从这里进入：[image]镇压应对措施

在反全球化抗议运动中，监狱声援战术取得了一些胜利，原因之一就是在组织大规模抗议活动的过程中，这些战术都是事先公开策划的。从理论上讲，你有可能在被捕后讨论并采用同样的团结战术，但在如此短的时间内很难得到其他人的认同。

最重要的是，要在情感上和精神上为被拘留做好准备。熟悉自己的权利和典型的警察谎言和诱导伎俩。练习一句话，比如："在我有律师之前，我只会给你我的名字和地址"。或者最自信地表达你不会和警察说话的原则。排练一下。让自己习惯于说出来。

12. 重申：最好任何时候都不要和警察说话

在你被释放后，你不必和给你打电话的警察、侦探或地区检察官交谈。向你的律师和你的队友们报告任何警察对你的接触或骚扰。

另外，不要做任何 "实际上等于" 和警察说话的事：不要在获释后和媒体交谈 —— 无论他们发表什么有你名字的文章，对警察来说都和与你直接交谈一样有用。在签署任何集体诉讼之前，先和你的律师谈谈—— 如果你的刑事案件还在进行中，有些案件可能会要求取证，强迫你作证，这可能会成为对你不利的证据。

[image]

返回：

一定践行良好的安全文化！并考虑如果警方没收了你的智能手机，可能会获得哪些关于你和你的团队的信息。更改你的密码。尽快把手机号码换成新的，这样来电就不会一直打到警察持有的号码上。

[image] 您可以点击右上角三个点 - "更多选项" - "查看原始内容"，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点

击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

以上这些建议会为您提供一个起点 —— 但不要完全照搬。新的抗议者可以问问前几代的抗议者，他们应对大规模逮捕的经历。时代已经变了，但其中许多教训仍然是相关的—— 包括一些我们无法在这样的描述的东西。

一定要随机应变！您了解的可能性越多，您的应变计划就越丰富，您就越容易做到冷静沉着 。

好运。

[image]
[image]

了解防弹衣：街头实战指南 S05E08

[image] 关键词	护甲 枪击 直接行动 街头 街头战术 防弹衣 防御
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月11日
[image] **Description**	行动安全性

愿我们都能活着看到更美好的未来。

- Table of Contents

摘要
曾经的 **Tute Bianche** 和 **Padded Bloc**
合法性
采购防弹衣
运动装甲
自己动手制作盔甲
对付刀子的盔甲
中世纪盔甲
软甲
材料
板式防弹装甲
板材
1、材质
2、尺寸
3、切割
4、曲线
单独使用与配合使用

创伤垫
自己动手制作防弹板
载具
隐蔽型装甲
这有多个好处：
公开型
MOLLE和其他固定点
DIY载具
装甲尺码
穿着防弹衣时中弹是什么情况
穿透率
防弹等级
NIJ标准
当前标准
即将到来的标准
防弹头盔
防弹盾牌
关于防割伤的说明

[image]

[image]

必须说，把街道拱手让给警察和暴徒最终只会增加所有人的危险。通过采取适当的预防措施，行动者可以减轻风险，同时继续采取行动，建设一个更美好的世界。

本集将回顾各种防护装备，探讨每种装备的优缺点，以便您能挑选出最适合自己的装备。您拯救的生命是您自己的。

重点关注三种类型的装甲：

1. 运动装甲，用于减轻豆袋弹和警棍等冲击性武器的伤害；

1. 软防弹装甲，或“防弹背心”，用于抵御手枪的伤害；

1. 板式装甲，用于保护您的重要器官免受步枪射击。

行动者面对的威胁模式（即您需要防范的风险）在不断变化。几年前，抗议者佩戴装甲的目的是为了防范拿着刀棍的暴徒；在BLM之初，主要威胁模型涉及警察使用各种冲击性武器；而到2020年夏天结束时，警察仍然在发射榴弹和胡椒球，但法西斯分子射击的实弹已经成为一个更紧迫的问题。

[image]

返回：[image]每一种变化都有原因，您需要及时抓取威胁信号 – 整体安全S01E05 - 紧贴时局

所有的装甲都涉及到优点和缺点。大多数装甲降低了机动性，机动性是抗议者对抗警察的主要优势之一，因为警察经常被官僚主义的指挥结构和沉重的装备所拖累。大多数装甲会让行动者脱颖而出，使到达和离开行动地点变得更加困难。有些装甲还会有法律处罚的风险。如果您是唯一一个穿盔甲的人那就很糟了，除非它可以被隐藏起来。不过，将穿戴盔甲正常化可以改变这点，而且穿戴盔甲的人越多，我们所有人就越安全—— 既不会受到直接攻击，也不会因为保护身体而被警察盯上。

哪种盔甲是合适的，会因情况不同而不同。在许多情况下—— 例如，当更高的速度或更低的曝光度是最重要的时候—— 最好还是不要穿盔甲。

装甲很容易给穿戴者一种虚假的安全感。在撰写这篇文章前不久，又发生了一起法西斯分子枪杀反示威者的事件，幸存者穿着防弹衣，但子弹进入他们身体的部位却没有防护。

没有人是铁打的，无论穿什么衣服。您需要记住这点。

[image] [image]

摘要

如果您想主要保护自己免受警棍和其他警用冲击性武器的伤害，可以

买一个滑板头盔，一些硬壳护膝，一些儿童护胫板穿在前臂上，可能还可以佩戴越野车胸甲或塑料击剑胸甲。如果您想增加更多的保护，可以考虑盾牌、全腿甲，以及为击剑运动员准备的 HEMA gorget—— 塑料或填充的颈部盔甲。盾牌的指南在本文的后面。

如果您想穿一些能保护自己免受手枪伤害的东西，可以买一件包裹性的IIIA战术背心。如果您担心的是刀子，可以多花点钱买一件有防刺功能的背心。

如果您想保护自己不受步枪子弹的伤害，可以买一个携板背心和一对III+防弹板。请注意这个会比较重，可能妨碍您的快读运动，也比较难隐蔽。

曾经的 Tute Bianche 和 Padded Bloc

不久前，美国和欧洲许多示威者面临的主要威胁是警察警棍的钝性冲击。作为回应，一些示威者 —— 尤其是意大利的 Tute Bianche—— 戴上头盔和衬垫，以保护自己的身体不受警察的拳头和棍棒的伤害。美国的一些示威者接受了这些战术，这被称为 “Padded Bloc” 。

https://youtu.be/BzZBLkhY5IM

今天的示威者仍然可以从当时制定的战术中学到很多东西，特别是在几乎没有致命暴力或攻击威胁的情况下可以部署这些战术。

从本质上讲，作为一种激进的非暴力反抗，Padded Bloc 战术最有效，其目的是延缓或干扰不准备升级到潜在的致命武力的对手。它们对于分散注意力和拖延时间比赢得进攻性胜利更有用，但它们可以在一个更大的战术和战略的生态系统中发挥宝贵的作用。

本集将主要关注能够抵御刀枪的盔甲形式，以扩大现代抗议者的选择范围。

[image] 反资本主义示威者反对2001年在意大利热那亚举行的G8集团首脑会议。

下面是一个视频，来自欧洲各地的示威者反对2000年在布拉格举行的国际货币基金组织和世界银行的首脑会议，其中包括一些采用 Tute Bianche 战术的示威者：

https://youtu.be/fAqbo_x2d0o

合法性

我们不是律师，您应该做您自己的本地研究。

在美国，联邦政府禁止暴力重犯拥有或穿戴用于抵御子弹的盔甲（在此称为“防弹衣”），除非得到雇主的特别许可。

除联邦法律外，美国各州都有自己的法律对防弹衣进行管制。在大多数州，如果被发现穿戴防弹衣，可能会受到额外的指控。在堪萨斯州，示威时也被禁止穿戴防弹衣。在康涅狄格州，你甚至不能把防弹衣运到你家里。关于未成年人是否可以拥有或穿戴防弹衣，还没有找到确切的答案。

防弹衣的合法性在不同的国家也有很大的差异。比如在加拿大的一些省份和澳大利亚的一些地区，您需要授权或拿到许可证才能穿戴。英国似乎没有限制平民使用防弹衣的法律。欧盟禁止用于“主要军事用途”的防弹衣，这意味着只有某些形式的防弹衣是合法的。幸运的是，在日本和香港，防弹衣似乎是合法的，但在阿根廷、巴西和泰国都是被禁止。

[image] 越野摩托胸甲

采购防弹衣

截至本报告编写之时，防弹装甲在美国已很难买到。不断加深的政治

危机使各方争相保护自己；大多数软甲和硬甲零售商都报告说，订单至少延迟两个月才能有货。建议您提前了解自己所需的产品，并留意交易 —— 或者甚至只留意产品有货的通知。

[image]

简单说，您不能等到危机真的加深了即将爆发了才开始准备装备。行动者社区应该长期预算此类工具，包括面罩、头盔等。

美国有一家装甲商叫红星防务。他们自己生产的III＋防护板价格不菲 —— 目前是300美元一副—— 而且零售的IIIA软背心价格也不低（225美元），但他们也出售比其他地方更便宜的防弹版和战术手套。目前他们的盔甲订单有4到8周的滞后期。这家公司是左翼，他们的目标不是利润，而是保护革命者的身体。

大多数防弹衣零售商的目标是三个市场的某种组合：警察和军事人员、右翼准军事人员、和私人保安（以及延伸到参与非法活动的人，比如黑帮）。只有少数零售商还在专注于保护平民和学童的安全，推广 “防弹背包” 和类似的产品。

到目前为止，快速周转防弹衣订单的最佳市场是eBay。新的IIIA防弹衣可以从英国和加拿大采购，随时可以发货；来自美国的剩余物资防弹衣也应该很快就能发货，不过这些防弹衣的存货量有所不同。大多数剩余物质都是将过期的凯芙拉纤维插入到新背心中的。

【注：凯芙拉是美国杜邦公司于1965年推出的一种芳香聚酰胺类合成纤维，发明者为波兰裔美国化学家斯蒂芬妮·克沃勒克。

凯芙拉极佳的抗拉性能，其强度为同等质量钢铁的五倍，而密度仅为钢铁约五分之一，因此在70年代初被用于替代赛车轮胎中的部分钢材。此外，凯芙拉不会像钢铁般与氧气和水产生锈蚀。】

对于剩余物资防弹衣的看法不一，但大多数情况下，它们被认为是可以接受的。因为凯芙拉纤维会因紫外线照射而退化，所以它有一个有效期 —— 通常是生产后五年。警察部门在五年后就会更换装备。但盔甲在很长时间后仍然有效。在我们看到的每一项测试中，过期的凯

芙拉防弹衣都能继续抵御所有额定的威胁。

不可能推荐使用过期的防弹衣，因为无法保证它们的安全性，但二手防弹衣的性能很好，而且比新防弹衣便宜很多。此外，具有讽刺意味的是，警察剩余物资防弹背心的零售商往往是最不针对右翼和警察市场的零售商。

您可以亲自到军队剩余物资商店购买防弹背心，特别是剩余物资背心。可以带着现金到商店去购买，如果能有熟人就更好了，可以要求不被记录的批量购买。

在 Armslist 上也有一个防弹衣的市场，它就像 Craigslist，后者是枪支的市场。看来一些有进取心的人，预计到当前的危机，已经囤积了很多装备，并直接出售。

但是，据报道，该网站上有很多骗子；如果您在该网站上购买任何东西，最好使用提供买家保护的服务，比如**PayPal**，而不是通过 **Venmo** 支付，因为 Venmo 没有保护。如果卖家不想支持买家保护，这本身就是一个危险信号。

[image]

有传言说，使用 ArmsList 的人被人陷害抢劫。考虑在白天在光线充足的公共场所见面，并带一个伙伴一起去，尤其是可以合法隐藏枪支的人。

您可能希望确保您的衣服和车辆不会泄露您的政治立场或其他有关您的细节。如果您使用现金购买，请在拿到物品后再付款。

在可能的情况下，向经过ArmsList 审核的卖家购买。

另一方面运动装甲仍然是现成的。虽然COVID-19使人们很难在旧货市场和二手商店里以便宜的价格买到运动装甲，但您通常可以以非常便宜的价格买到二手装甲。在美国，也许能在枪展上找到高质量的护膝和护肘，因为伊拉克和阿富汗战争中退役的军事装备充斥市场，使

价格下降。

[image] IIIa级背心

运动装甲

运动装甲提供了一种廉价而合理有效的方式来保护自己不受冲击性武器、警棍以及某种程度上的刀子的伤害。

但它不能保护您不受枪击伤害。您通常可以从二手货源中获得；其中大部分可以隐藏在衣服下面，这点非常可取。它在法庭上可能会比弹道装甲看起来更安全，不至于让您因为一个背心吃官司。

它是合法的，很多的人穿它 —— 它不太可能引起额外的指控，而如果您穿着专业的防弹装甲，就有可能因此被指控。法庭会据此声称您“持有犯罪工具”。

运动装甲的基本原理是 “硬/软” 的防护模式。外部坚硬的外壳（通常是塑料）承受武器的冲击，防止穿透，并将冲击力分散在广阔的表面区域。在外壳下面，柔软的填充物吸收冲击力。

有效的盔甲都需要这两个部分。例如，中世纪的钢铁盔甲，依靠厚厚的绗缝布层来减少打击的冲击力。一些现代运动装甲缺乏硬壳，包括加垫的衬衫和裤子以及拳击头盔；这些都不太适合现代行动主义的目的。

[image]

防弹装甲是为了保护您的重要器官不受枪击，而运动装甲则是为了保护您身体的更多部位—— 例如，肩膀、前臂或关节，这取决于盔甲本身的设计。对付警方的冲击性武器，这一点至关重要。

警察接受过训练，大多数冲击性武器都直接会瞄准您的肚脐或以下部位；他们通常特别针对膝盖或四肢。然而，警察也经常用冲击性武器直接射击人们的胸部、背部或头部，并将警棍刺入胸部或腹部，或者

挥动警棍殴打人们的背部或头部。

当务之急是保护好自己的头部。之后，您可以考虑护膝，因为对膝盖的冲击比对身体其他大部分部位的打击更具有致残性。

当冲击弹药致人死亡时，通常是因为它们击中了人的头部或胸部；胸部受伤可能会打断一根肋骨，从而刺穿肺部或心脏。这种情况不常见，但是，保护胸部绝对是个好主意。一些预计会与持棍攻击者近距离接触的人，也需要戴上前臂护具，通常是重新利用护胫板。这些护具可以用来阻挡棍棒或警棍的打击，尽管这种护具很难保证全面的安全。

[image] 这是击剑运动用的护胸装甲

自己动手制作盔甲

您也可以自己制作有效的盔甲，虽然二手运动装备往往很便宜，以至于没有必要这样做。但如果您预测购买会被记录身份，或者的确买不到，那自己做就是好主意。

[image]

返回：[image]匿名购买

在自己动手制作装备时，要确保遵循硬/软质模型。对于外壳，塑料是最轻的，一般来说也是最好的，但金属板也可以—— 橡胶、木头甚至厚厚的杂志都可以。我们知道有一个抗议者戴着用旧车牌做的前臂护具，很帅的。

橙色的交通锥材料虽然不是特别坚硬，但聊胜于无，而且往往容易买到。您还可以用很多方法重新利用塑料水桶。我们遇到了一种特别有前途的方法，用5加仑的水桶制作简单的胸甲，虽然对于我们的目的来说，它需要在后面垫上泡沫。

对于“软”层部分，闭孔泡沫通常是最好的东西。瑜伽垫材料通常是

便宜而有效的。大型超市卖的露营垫的蓝色泡沫被那些自己制作运动装备的人认为是便宜的和好的材质。即使是包装泡沫也可以用。试着用喷胶，或者更好的是用胶浆来连接。

有人用以下方法免费制作定制盔甲。

[image] 蓝色泡沫垫

从垃圾箱里捡那些丢弃的旧床垫和5加仑的塑料桶，将桶切成与要覆盖的身体部位（大腿、胫骨、手臂等）大致匹配的条状物，然后将条状物放入烤箱中低温加热。注意温度，不要融化塑料 —— 只要把它软化 —— 就可以了。有些人喜欢用捡来的烤箱来做这个，而不是用自己煮食物的烤箱。同时，把床垫上的泡沫撕下来，然后用胶带暂时贴在要覆盖的身体部位。将塑料从烤箱中取出，然后在泡沫上成型，一旦冷却，就用喷胶或胶浆将泡沫贴在塑料内部。

[image] 胶浆

对付刀子的盔甲

在制作DIY塑料防刀盔甲的实验中，我们发现任何坚硬的塑料板都会有实质性的防刀效果，但这种盔甲需要相当厚的塑料才能防刀。

一位测试者可以做到避免让刀子刺穿大多数塑料板，但另一位测试者几乎能让刀子刺穿放在他们面前的每一块塑料板。不过，在混乱的斗殴中，大多数刺伤不会是全力的，硬塑料层即使不防刀，也能提供实质性的阻力。这种程度的保护仍然是割伤疼痛和刺破器官之间的区别。我们还没有对运动装甲进行专门的防刀和防撞击武器的测试。

[image] 防刀割的袖套

中世纪盔甲

中世纪的盔甲一般都是按照与现代运动盔甲相同的原理设计的：硬壳下有衬垫。今天穿中世纪盔甲进行运动的人已经做了很多工作，将中

世纪的盔甲更新为现代用途。其中大部分可以适应抗议中的使用。

钢制铠甲往往比塑料铠甲更重；它比塑料铠甲的主要优势是抗切割和抗砍伐。这对于那些希望保护自己不受钝性冲击的示威者来说不那么重要。

穿着和了解中世纪盔甲的两个现代团体是“创意不合时宜协会”（SCA）和那些研究“欧洲历史武术”（HEMA）的人。两者都倾向于穿戴钢铁和塑料盔甲的组合，但**SCA**特别开发了**DIY**塑料盔甲，旨在保护人体的各个部位。他们的设计很可能对示威者有效。

我们不能推荐钢制头盔，因为警方使用的冲击弹药的威力远大于古代冷兵器，钢制头盔的变形（凹陷）会危及佩戴者的生命安全。我们已经研究了这个假设，但还没有进行测试。

中世纪的盔甲也太吸睛了。如果您公开穿戴它，必然会引起注意。当然，无论是在历史上还是在现代，盔甲往往被设计得像衣服一样，或者穿在衣服下面。别看电影里面那些古人穿着闪闪发光的铁皮罐子到处跑，这种想法基本上是不符合历史的。

中世纪的盔甲并不是防弹的 —— 至少不是特别防弹的。为了有效地抵御子弹，钢铁必须至少有1/4英寸厚，并且由一种几乎难以加工的硬合金组成。

[image] 2017年一位示威者反抗法院对警察和凶手有罪不罚

软甲

软甲背心比较轻，适合奔跑，隐蔽性好，对手枪子弹有效，对刀子也有不同程度的效果。理想的情况是，您需要一件IIIA级的防弹衣，尽管II级防弹衣通常在剩余物资市场上更容易买到，而且聊胜于无。

II级可以防备一般的9毫米子弹，但不能防备枪支爱好者常用的“自卫”9毫米子弹。防弹衣经常很昂贵（有些可以用250美元左右的价格

买到新的，但大多数要400美元以上）。二手的或剩余物资的防弹背心（通常仍然是200美元以上）可能会提供比新的更少的保护，虽然这是值得商榷的，也难以测试任何给定的背心。对于大多数担心手枪射击的示威者来说，软甲可能提供了保护、重量的优势和隐蔽性的最佳平衡。

软装甲采用多层坚固的塑料和内衬织物构成。每层都能吸收子弹冲击力，直到最终被织物本身吸收。

大多数软甲使用凯芙拉纤维，但 Dyneema 和 Spectra（超高分子量聚乙烯的品牌名称，另一种塑料纤维）是一种更新更强的材料，在各种类型的装甲中越来越常见。

这种原理在盔甲中已经使用了几千年。中世纪的 Gambeson 是一种由多层亚麻布制成的绗缝织物；虽然那些有能力这样做的人在其他盔甲下穿着它，但一些战斗人员—— 如起义的农民—— 单独穿着它。它对箭特别有效，因为分层织物特别擅长阻止穿透。

当您选择软背心时，必须在 “环绕式” 背心和只从正面或背面保护您的背心之间做出选择，“环绕式” 背心有大面积的保护性插片，可以保护您的侧面以及您的前胸和后背，而 “环绕式” 背心的功能几乎与板式装甲相同，只是用软织物装甲代替了板子。除了价格之外，几乎在所有方面，环绕式防弹衣都是可取的—— 大多数最便宜的IIIA装甲只保护您的正面和背面。

和防弹板背心一样，软质背心通常有 “隐蔽” 和 “公开” 两种样式[见下文]。但由于软背心比背板的主要优点之一是可以隐藏，所以似乎没有什么理由考虑必需穿在外面的软背心。

[image] IIIa环绕式背心衬里

材料

软背心有两种不同类型的塑料纤维：芳纶和超高分子量聚乙烯。任何一种都不会错。芳纶纤维（如 凯芙拉）是一种略显老旧的技术；在相

同的保护水平下，它们更重。而超高分子量聚乙烯纤维（如Dyneema）是更精细、更新、更轻、更抗紫外线、但更不耐温度变化的纤维—— 这意味着当枪直接抵住背心时，它们不太能阻止“接触式”射击，因为纤维会熔化。关于这是否是一个重要的问题有一些争论。

芳纶纤维是防弹背心中最常见的塑料类型。最受欢迎的品牌是杜邦公司生产的凯芙拉纤维。芳纶纤维是第一种强度足以制作成防弹衣的材料。另一个用于装甲的芳纶纤维品牌是帝人芳纶（以前称为Twaron）。

芳纶纤维在紫外线照射下会分解。防弹衣的外壳一般可以保护它们不受影响。

超高分子量聚乙烯 (UHMWPE，有时简称PE) 是一种塑料纤维，越来越多地应用于各种类型的装甲。软质背心由分层织物制成；硬板常以它为背板或完全由它制成；现代军用头盔由它代替芳纶纤维制成。按重量计算，它的强度比芳纶纤维高，所以可以把盔甲做得稍薄、稍轻。

装甲中使用的超高分子量聚乙烯纤维最常见的两个品牌名称是Dyneema（DSM制造）和 Spectra（Honeywell制造）。

虽然超高分子量聚乙烯本身并不具备抗紫外线的能力，但它可以很容易地制造出来，而且被认为比凯芙拉的对紫外线稳定性大大提高。我们无法找到关于 Spectra 的可比信息，除了它被宣传为比许多其他纤维（可能包括芳纶）更耐紫外线之外。

超高分子量聚乙烯的熔点比芳纶低得多；有人猜测它会因此受热而降解。我们发现有一家制造商将他们的背心点燃整整一分钟，然后进行测试，发现它们能继续阻止子弹。同一家制造商还对他们的防弹衣进行了接触射击测试，尽管我们不知道是否所有超高分子量聚乙烯防弹衣都会产生同样的结果。

[image]

在任何情况下，一般不建议将任何含有超高分子量聚乙烯的软背心放在任何可能超过华氏180度的环境中；并且它们仍然被认为比芳纶纤维背心更容易在接触性射击中受害。

板式防弹装甲

如果您想保护自己不受步枪的伤害，背板几乎是唯一的办法。对于板式防弹装备，您需要两样东西：板子 —— 织物背心作为载具，用来装硬板。一般来说，您需要III级以上的板子，最好是陶瓷和PE（聚乙烯，通常是上面提到的UHMWPE）的组合。侧板很可能是矫枉过正了，不必要的重量和费用，四级板也是如此，它是保护性最强的装甲。

[image]

请注意，硬板表面上比其他形式的装甲更防刀，但公开穿戴的版式防弹衣非常明显，一个坚定的攻击者只会瞄准您没有保护的地方。

板式装甲只是为了保护您胸部最重要的区域，这个区域有时被称为"杀伤盒"。大多数枪手都被训练成瞄准"身体中心部位"，因为它是最大的目标，也提供了最多的漏洞。除了头部伤口外，身体其他地方的伤口不太可能杀死你，所以大多数装甲系统并不优先预防这些次级危害的伤口。

板式防弹装备和软背心一样有"隐蔽"和"公开"两种型号，隐蔽的设计在衣服下面穿着，公开的设计在外面穿着。

板材

先挑选板材，然后再为其搭配载具，这被认为是一种好的形式，不过您也可以按相反的顺序进行。

关于板材，有几件事需要考虑，包括材质、尺寸、切割和曲线。

1、材质

板材由一系列可以阻挡子弹的东西构成。这里将介绍软板、钢板、陶瓷板和PE板。

软板是由上面防弹衣一节中讨论的防弹布层层叠加而成的。如果您想寻求模块化，可以保留一对软板，当您想要一个更轻的装甲时，可以插入您的防弹板载具中 —— 就是专门携带防弹插板的轻量化背心，而不是硬板。

优点：轻巧，灵活。缺点：防护性差。

钢板是最常见的，但正在走向过时。钢板是钢质的，厚度约为0.25英寸。最常见的钢合金是AR500，是一种特别坚硬的钢。主要用于装甲、犁刀、建筑和采矿设备等。钢板每块很容易就有8、9斤重。(有一个装甲制造商就叫AR500，他们生产各种类型的装甲)。

现在钢板不太受欢迎了，因为陶瓷板的价格越来越实惠。钢板实质上更重。 当从一定角度击中时，它们会导致子弹跳弹，并且能够导致“破碎”，即 细小的钢铁碎片会飞溅。垂直角度的飞溅是最主要的麻烦，因为它可能会朝您的脸飞去。

唯一值得考虑的钢板有“防飞溅涂层”，这通常是卡车上用的那种衬垫涂料相同的东西（如喷涂的 Rhino Liner），尽管我们相信一些制造商使用玻璃纤维套管代替。许多制造商提供了关于您希望涂层有多厚的选项。厚的涂层对前板比后板更重要。在出现更多的垂直飞溅之前，涂层通常会保护佩戴者免受两到三次撞击。

现在陶瓷板的价格已经很便宜了，钢板的主要优点是比陶瓷板更薄，在同一弹着点上更能承受更多的子弹。

陶瓷板有时被称为复合板，因为它们通常不完全由陶瓷制成。它们的工作原理是在撞击时分解，吸收大部分子弹的冲击力，然后由第二层

阻止子弹的穿透力。曾经，这第二层通常由钢组成，但现在最常见的是聚乙烯。陶瓷板的重量一般在五到六磅之间，厚度在0.75英寸到1英寸之间，便宜的陶瓷板往往更厚更重。

按成本和功效递增的顺序，最常见的三种陶瓷是氧化铝、碳化硅和碳化硼。氧化铝需要更厚更重才能提供与碳化硼相同的保护能力，但价格却要便宜很多。买多套氧化铝板分发给朋友，可能比买一套只有自己才能戴的花哨轻巧的板子要更好，不过更薄的板子更容易隐藏。

有人担心陶瓷板可能会因为粗暴的操作而退化，但目前的观点是，这种担心被夸大了。

陶瓷板的一个危险是，为了节省成本和降低重量，大多数制造商沿着板子的边缘使用泡沫而不是陶瓷。这一点通常在项目描述中会提到。我们处理的一个板子的边缘有一整英寸的泡沫—— 把一个表面上是10×12” 的板子减少到 8×10” 的尺寸，完全有效—— 尽管PE在陶瓷下面轧边，它一般被认为是IIIA级的（足以阻止手枪子弹）。红星防务公司宣传的是轧边弹道陶瓷板。

推荐陶瓷板是因为它们实质上更轻，而且不存在飞溅的问题。然而，它们将无法像钢板那样经受得住多次连续的射击，而且由于它们的刚性较差，它们更容易发生背面变形（凹陷），从而将更多的冲击力传递给佩戴者。您可以通过使用创伤垫来减轻这种危险，创伤垫本质上只是额外的填充物。

[image] 多次冲击后的陶瓷板

PE（聚乙烯）板是完全由超高分子量聚乙烯制成的板材。与软装甲一样，它依靠多层薄板。与软甲不同的是，这些层是热合在一起的。当子弹击中板子时，它每次都会将每一层打散，这种分层每次都会吸收冲击力。因为这个过程会造成相当大的背部变形，所以大多数PE板都有一层泡沫作为内衬支撑。

PE板比其他硬板轻得多，通常不到三磅。它们在水中也具有浮力。但它们的厚度要大得多（1–1.25英寸），因此隐蔽性较差。最重要的是，我们还没有找到任何等级高于III级的板子
——

似乎穿甲弹可以直接穿透塑料层。由于AR-15是美国最常见的步枪威胁，而一些可用的AR-15弹药选项可以穿透III级板，因此无法确保它们的安全性。

[image]

在您的国家也许不同。先了解下您的国家的镇压部队和暴徒最常使用的武器是什么型号的。

任何含有PE的硬装甲，如陶瓷或独立PE，都不应该暴露在华氏180度以上的温度下。

[image] UHMWPE板

2、尺寸

粗略的说，一块板子至少应该保护您从锁骨到肚脐上方几英寸，从一个乳头到另一个乳头。

有两个不同的尺寸标准在美国使用。我们称它们为民用和SAPI。

民用板是最容易遇到的，有8×10″、10×12” 和 11×14″三种尺寸。10×12” 的尺寸是最常见的。

SAPI（Small Arms Protective Insert）是军用保护板的缩写。SAPI板有一个非常特殊的切口（SAPI切口），但有五种不同的尺寸：特小号（7.25×11.5″）、小号（8.75×11.75″）、中号（9.5×12″）、大号（10.25×13.25″）和特大号（11×14″）。

[image]

测量板子尺寸的最佳方法是测量您的身体，然后选择最适合您身材的板子尺寸。当然这不是牛仔裤，您可能无法获得所有可能的尺寸。差不多就行。

[image] 一块完整的板子

3、切割

板子有很多不同的形状：全切割、SAPI、射手型和泳者型。这些之间的差别不大，每个切口（除了SAPI这个军用标准在外）都因厂家不同而不同。虽然大多数板子都是成对出售的，但其中很多是混搭的，一个普通的SAPI切割后板和一个较深的射手型切割前板。

全切割板基本上是矩形，四角被磨圆。它们并不常见，但可用于侧板或背板。它们可能不适合许多载具。

SAPI板是标准的军用硬板。他们有一个近45度角从顶部的每个部分切割。SAPI板效果比较好，能提供大量的覆盖面。实际的军用SAPI板不直接对外销售，但制造商以 “SAPI cut” 的方式销售板子。

[image] SAPI防护板 射手型

射手型的板与SAPI板类似，但边角处的切口略多。手臂上的切口角度是为了能更好的移动。

[image] 射手型切口的防弹板

泳者型的切割板在远离顶角的地方有较深的切割，形成隐约的水滴形。这就牺牲了对流动性的保护。一些胸部较大或曲线玲珑的身材会觉得泳者型板子最舒服。

[image] 泳者型钢板

4、曲线

板材可以有三种不同的曲线风格：平面、单曲线、多曲线。同样，每个品牌对这些都有自己的解释。

- 平板就是平的。大多数人不喜欢平板，虽然有些人戴着，特别是在后背上。有时候平板比较便宜。

- 单曲线板是最常见的。这些板子在垂直轴上是弯曲的，以便更

好地包裹住您的躯干。

- 多曲线板以多种方式弯曲，以更好地适应制造商认为的大多数客户的身体。这些通常是优选的，特别是对于胸部比较大或有啤酒肚的人。它们通常更贵。并非所有制造商都提供这种选择。

[image] 这是多曲线板

单独使用与配合使用

我们讨论过的大多数防护板都是独立式的 (SA 或 STA) 。这些板子的设计是为了使其自身达到额定水平。

也有可能获得结合使用 (ICW) 板子。这些板子通常更薄更轻，但只有与 **IIIA** 软背心一起穿时才能发挥其额定水平。

后者的模块化系统有很多值得推荐的地方，但您必须采购一件带有插板的防弹软背心（通常比较贵），否则就需要在背心上穿一个板式载具。ICW板比较难遇到。整个系统可能会更贵。

这种样式曾经是比较流行的军用样式，因为它提供了更多的保护，但目前的趋势更倾向于机动性而不是保护，也就是更方便运动，军队似乎正在转向使用独立的板子。

创伤垫

买盔甲的时候，可能会遇到 “创伤垫”。这个词其实有两种不同的含义。在独立的防护板之前，ICW被称为 “创伤护垫” ，被插入防弹衣上的套子中，以增加其防弹等级。但现在，“创伤垫” 通常是您放在硬板后面的非防弹泡沫插片，以软化冲击的钝力创伤。

创伤垫的价值是有争议的。它们对陶瓷板似乎比钢板更重要。人们用瑜伽垫泡沫材质自制创伤垫的方法也越来越流行。

我们没有足够的信息来对这场争论的任何一方下定论，但可能值得去买或制作创伤垫，特别是如果您有陶瓷板的话。它对防治伤害的作用无法期待太多，有些人穿它们只是因为它们使能盔甲更舒适，尽管它们确实增加了费用和厚度。

自己动手制作防弹板

是可以制作DIY装甲板的。这可能是作为最后的手段才值得做。YouTube 是一个神奇的仙境，充满了人们测试各种DIY形式护甲的视频。有的很容易制作；有的则是劳动密集型的。有些是负担得起的；有些是比较贵的。我们没有亲自测试过DIY防弹衣，所以无法推荐，但在有些情况下，您需要装甲而又买不到的时候，DIY可能是唯一的办法。技不压身，多学点有好处。

我们见过两种常见的方法。第一种方法是将很多很多层的凯芙拉纤维（更好）或玻璃纤维（更便宜）与树脂复合在一起。这是劳动密集型的，而且不一定便宜，但它可以让您把板子做成各种形状。关于什么样的树脂效果最好，有点争议；有人认为，使用较少的树脂可以使板层在撞击时分层，吸收更多的冲击力，这一点令人信服。

第二种方法实质上更简单，而且通常更便宜，包括将陶瓷板—— 使用最硬的地板砖—— 与不同厚度的钢和橡胶分层结合。这种方法似乎可以做出更坚固的装甲，不易发生背部变形。有人认为，陶瓷马赛克地砖具有更好的抗冲击能力，也有人说单块较大的地砖能更好地吸收冲击力。氧化铝陶瓷板很容易采购，中国特别多。

有些人将这些不同的方法以各种方式结合起来。

https://youtu.be/xcLkyXzqNU8

有个人用牛奶罐和回收的高密度聚乙烯做了一块又厚又轻的板子，看起来大概是2级或3A级。

https://youtu.be/MI9F5BEOpJs

另一个人则证明了厚厚的超高分子量聚乙烯板作为装甲没有任何用处。

https://youtu.be/ios2jb9wtTs

我们见过的最便宜、最奇怪的DIY板子是用一元店的廉价物品做成板子：装满石头和胶水的烤盘，用一本精装书作为弹片防护。这能阻止一些步枪子弹，但不是很多。

我们交谈过的一个人使用在废品收购站找到的适当强度和厚度的钢材切割钢板取得了一些成功。太硬的钢材会在撞击时破碎；太软的钢材会被穿透 —— 如果子弹真的穿透板子，可能会留下额外的锯齿状金属碎片。如果您要采取这种方法，获得足够的额外材料来测试这些板材绝对是至关重要的。您可以用角磨机将钢板切割成所需的形状。**DIY**钢板绝对应该有创伤垫的支持。

https://youtu.be/ee7TPp6mJIs

如果可能的话，您应该买到工程良好、经过正确测试的装备。如果做不到这一点，最好自己对自己制作的装备进行彻底的测试。过程是这样的：

1）广泛研究项目所涉及的核心概念，了解注意事项、潜在的失败点、和潜在的失败原因。

2）制定一个您希望完成的最小可行的产品标准。

3）确定最基本的测试条件，尽可能多的排除变量。

4）开发初始原型。

5）测试初始原型。

6）拆解原型，以确定哪些是成功的，哪些是失败的，并确定失败的

原因。

7）利用测试中获得的知识建立下一个原型。

8）重复进行。

9）一旦您达到了最低限度的可行产品标准，就开始在更加苛刻的条件下进行测试 —— 不同的温度，使用不同的攻击形式，等等，以确定弹性和故障点。

对于这样的项目，请确保您有机会直接参与最终的制作流程，并且合作者知道如何安全有效地使用必要的工具。适当的工具将使生产和测试速度更快；它们还可以帮助确保标准化的结果。

载具

很多厂商会把载具和板子作为一套卖给您，这样您就可以直接用了。否则，您将不得不选择一个载具来安装您的板子。要注意挑选一个能接受您打算佩戴的特定尺寸和裁剪的板子载具。

载具一般由两部分组成：背心本身，套在您的头上，还有一个褡裢——— 连接您身体前后板的魔术贴带。

载具有两种主要样式，即 隐蔽式和公开式。

[image] Slickster，一种受欢迎的载具

隐蔽型装甲

隐蔽型的设计是为了提供在其他衣服里面穿戴的选择。它们往往没有那么多的小袋和环以及其他战术装备选项。对于抗议者来说，隐蔽式

装甲可能是最好的选择。在宽松的黑色衣服下的隐藏它们不太可能被发现是防弹衣，特别是在黑暗中或大量的人群中。

这有多个好处：

首先，也许是最重要的就是，警察不太可能把您标记为一个麻烦制造者，否则警察很可能将您作为逮捕或其他暴力的目标。

同样重要的是，持枪攻击者也不太可能针对您。对于枪支，隐蔽式装甲的主要论点之一是，训练有素的攻击者会首先瞄准已知的威胁。基本上，如果有人走进一家商店并开始射击，他们很可能会首先瞄准任何他们看到的持枪者。

同样的原则也适用于盔甲：枪手更有可能认为穿戴盔甲的人是一种威胁，因此会首先瞄准这样的人。

此外，如果枪手知道您穿着盔甲，他们可能会故意绕避您受保护的地方而向您没有保护的身体部位开枪。外穿的防弹衣是为士兵设计的，而特种部队（spec-ops）则更有可能因为上述原因穿上隐蔽的防弹背心。

您可以模块化地穿戴隐蔽型的防弹背心，可以选择换上额外的小袋和褡裢。

不幸的是，便宜的陶瓷板往往太厚，以至于隐蔽型穿戴的难度大大增加。如果隐蔽性是您的首要任务，可以考虑购买更贵、更薄的陶瓷板。虽然目前还不能推荐钢板，但那也是比较薄的。

公开型

相比之下，公开型装甲的设计是作为最外层的穿戴，并作为悬挂装备的平台。传统上，这意味着枪支，弹夹，通讯设备，急救用品，以及

其他任何士兵需要的东西。我们不是士兵，我们是抗议者。

当然，对于某些人和某些目的来说，公开型的防弹背心仍然有其存在的价值。它们传递着好战和充分准备的信号，它们可以使盔甲的使用正常化。颜色鲜艳的公开型防弹背心经常被第一反应者和其他需要保护自己但又想表明自己是非战斗人员身份的人穿着。

另外，可以将装备挂在背带上，会很方便，比如无线电通讯设备和充当街头医生的救伤设备。

[image] 一个公开型的防弹板载具

MOLLE和其他固定点

军事和战术装备通常很容易通过缝满织带的环状物来识别。这就是所谓的MOLLE(模块化轻量级携行装具)：一种军事系统，旨在允许各种附加的小袋、背包、护套等。

有些MOLLE是激光切割的，特别是在隐蔽的载具上：在最外层的织物上切割了槽，而不是用织带环。

钩扣（魔术贴）固定点在战术装备上也很常见，用于连接士气徽章甚至小袋。士气徽章贴片包括军队用来指定单位的各种徽章和标志，也是有战术意识的平民用来表达政治立场和亚文化归属的标志。

一些特定的制造商也使用其他样式的固定点。

对于大多数隐蔽防护板载具来说，固定点是不必要的。

DIY载具

对于任何一个有缝纫经验的人来说，制作防护板载具都是一件相当简

单的事情，因为它本身并不是一个弹道产品。建议任何有志于制作载具的人都可以找一个简单的成品载具来仿制。

您可以用织带制作肩带，500D Cordura 似乎是背心本身最常用的面料。大多数指南建议每条缝线都要用双针或三针。

板子要装入前后垫的底部，一般用大方的钩扣固定。

装甲尺码

如果您的防护板载具很合身，护甲上方应该在您的锁骨处。

[image]

穿上护甲后，抬起手臂，扭动身躯，确保整个装甲能随身体移动，不能说您的身体在动，背心不动，那就太松了。

深吸一口气，确保不会太紧，最多在肺部完全扩张时，应该感觉很紧。

然后通过做一个跳跃动作或其他运动项目来测试是否合适，以确保载具上没有任何东西因为您的运动而移动或脱落。

这适合不同体型的盔甲。

大多数装甲的设计都是为了适合体格健壮、运动型的男性。您离这一类别越远，您可能会在安装护甲方面有更多的麻烦。要获得小尺寸的盔甲和胸部比较大的体型的盔甲可能特别具有挑战性。

软质防弹衣的宽容度大大高于板式载具，但对于那些曲线较多的人来说，仍然可能不太舒服。一些盔甲制造商专门设计了适合曲线身材的软甲背心。虽然我们在eBay上看到了一些剩余物资的“女性”马甲，

但这些马甲在低价位上不太可能找到。

一般来说，小号的防弹背心似乎很难在剩余物资市场上找到，因为这些剩余物资往往来自于警察部门，那些经过体能训练的家伙，体型比较大。

板式载具为有胸的人提供的选择就更少了。我们能够找到的最好的选择是买一个多曲线的泳者切割的前板，并穿上紧身运动胸罩或束胸。

同样，板子的尺寸也不会适合所有的人。似乎大多数大个子的人都会穿他们能穿的最大的板子（通常是11×14″），即使它覆盖的躯干依旧较少。

穿着防弹衣时中弹是什么情况

关于穿着防弹衣时中弹会对人体造成什么影响，有很多自相矛盾的信息。

[image]

如果您穿着软甲时中弹，冲击力仍然会击中您，并会对您造成伤害，不过由于冲击力被分散在更大一些的区域上，所以伤害一般都是相对轻微的。

根据一项研究，85%的人在穿着额定冲击力合适的防弹衣时中弹，没有受到伤害或受到轻微擦伤等轻伤。然而，一位急救人员说，他们治疗过的那些穿着防弹衣中弹后幸存下来的警察，形容就像被棒球棍全力击打那样。

防护板则完全是另一回事。穿着板甲时中枪，是否受伤和死亡是很有争议的。我们亲自和专家交流过，看到的测试和研究也是相互矛盾的。

在一般情况下，如果您穿着的装甲是为您所经历的冲击力额定的，您不太可能遭受重大伤害。除非您失去平衡，否则您不太可能被击退或翻倒。特别是钢，能有效地将子弹的力量传递到大面积的表面，将传递给穿戴者的力量降到最低。陶瓷板装甲的变形比较明显，但这种影响可以通过创伤垫降到最低，它应该不会对穿戴者造成惨重的伤害。

然而，并不是所有情况都一样。人们在穿着盔甲时，当子弹击中他们时，确实会造成肋骨断裂和其他钝器型的伤害。

根据体重的不同，人们可能会经历不同的冲击。较大的钢板可以将冲击力分散到较大的区域。

[image] 与防弹板覆盖有关的胸部解剖图

穿透率

弹道学是一个非常复杂的课题。我们与一些工程师和战术爱好者讨论了如何理解穿透的风险。

广义上讲，步枪的穿透力比手枪或霰弹枪要强得多。它们也被认为是更致命的 —— 虽然枪支暴力是一个高度政治化的主题，数据经常被歪曲以支持一种或另一种立场，而且我们发现关于根据口径宣称的杀伤力的报告是相互矛盾的。唯一的例外是.22口径的步枪，这种步枪常见于射杀小猎物和初学者，在穿透能力上比其他步枪更接近手枪。

装甲穿透力与整体威力（子弹传递给目标的动能）截然不同，整体威力与“阻力”（中和威胁的能力）不同。对于速度较快、“截面密度”较大的子弹来说，穿透力较强 —— 也就是说，相对于其宽度来说，这种子弹更重。较细的子弹比相同质量的大子弹更锋利，穿透力更强。穿甲力和阻击力实际上是相互作用的：在撞击后出现蘑菇状或碎片的子弹会造成更严重的伤口，而更有效地保持形状的子弹则更可能穿透装甲。

大多数穿甲弹的工作原理是使用钢或其他坚硬的弹芯，这种弹芯比铅弹更能有效地承受冲击。在美国，这种弹药一般不向平民提供，但军

队和警察都可以使用。这使得民兵团体和其他非国家行为者不太可能用这种弹药来对付示威者。它不被警方普遍使用的原因有很多：首先，它有更大的风险，可能会贯穿目标人，无意中击中其他人，这就是所谓的过度穿透；其次，中空弹（击中后会爆炸）对杀死非武装目标更有效，比如警方通常试图谋杀的普通公民。最常见的例外是7.62x54r钢芯子弹，它有显著的穿甲能力，50口径范围内的任何东西都可以穿透，但这种子弹不可能在抗议活动中遇到。

有两种子弹值得了解，因为平民可以获得，而且很可能被试图伤害示威者的非国家行为者携带。

第一种是钢头(非钢芯)子弹，一般称为 “绿头” 子弹。这些子弹是为军队设计的，在远距离上具有更高的准确性和穿透力，但它们在民用中也很常见，特别是在AR-15中。

第二种是 “＋P” 风格的子弹，一般是9毫米—— 最常见的手枪子弹—— 虽然不是所有的9毫米子弹都是＋P。这些子弹不是为穿透装甲而设计的，而是装填了更多的火药，提供了更大的威力，因此具备更有效的穿透力。

[image]

这两种威胁都可以通过适当的和可用的防弹衣来阻止，比如上文中推荐的。 值得注意的是这些威胁本身，以便了解为什么您可能需要一个适当的装甲水平 。

较旧的和较便宜的软防护背心可能会阻止大多数9毫米子弹，但不能阻止枪支爱好者通常携带的＋P子弹。

[image] 绿头子弹

防弹等级

护甲可以根据几种不同的标准进行测试，以确定其功效。对于在美国销售的产品，目前最常见的是国家司法研究所（NIJ）的标准，本文中一直使用的就是该标准。这些标准是以美国执法部门为中心设计

的。许多其他国家都使用NIJ标准为平民提供的装甲。世界各地也有其他标准在使用。

美军不使用等级评定，而是提供必须达到一定门槛的特定装甲物品。这些测试并不是“这种装甲能防手枪吗”甚至不是”这种装甲能防9毫米手枪”这么简单。这些评级指定的是具体的子弹，细致到它的成分是什么和装填的火药有多少。

[image]

同样，简而言之，如果您正在寻找软装甲，您应该希望它的评级是**IIIA**。

如果您要找的是硬装甲，您应该希望它的等级至少要达到**III＋**，

如果是为了保护您免受常见的钢头**AR-15**子弹的伤害，则要达到**“III级特殊威胁”**。

[image] 9毫米 Luger＋p 弹药

NIJ标准

NIJ标准会不时地进行修订。

当前标准

I级：这一级别不再是标准的一部分。它可以抵御一些.22lr(小型猎枪)子弹和.380acp(手枪子弹)。

IIa级：它可以抵御一些手枪子弹，包括一些9毫米、.40和.45的子弹。

II级：可以抵御更多的手枪子弹，包括9毫米以及一些.357子弹。

IIIa级：这可以防止几乎所有的手枪， 包括更多的.357子弹和.44 magnum子弹。

III级：这个级别的额定值可以阻止大多数 7.62x51mm 北约子弹，一种常见的军用子弹。它对AR-15的额定值不高，但可以阻止很多AR-15的子弹（5.56或.223，大致相同）。

IV级：这个级别的额定值可以阻挡30.06穿甲弹—— 二战时期的战斗步枪发射的子弹，这种子弹如今在狩猎中仍然很常见。

即将到来的标准

新的 NIJ 0101.07标准可能很快就会在某个时间点发布。此次修订将解决现行体系中的主要漏洞，如III＋填补的空白。它将用两个独立的类别取代数字系统：HG（手枪）和RF（步枪）。

HG将有两个级别HG1，它将映射到现有的II级，HG2，它将映射到现有的IIIA。RF将有三个级别，RF1将映射到现有的II级，RF2将填补目前III＋级的空缺，RF3将映射到现有的IV级。

防弹头盔

大多数防弹头盔的等级都是IIIa级，是用来阻挡手枪子弹的。

一些较新的军用头盔可以阻止一些步枪子弹，有时是从远距离的射击。

还有一些头盔可以使用插片来增加头盔的防护等级，不过这些插片并不常用，因为大多数士兵似乎更喜欢减轻重量而不是额外的防护等级。

IIIA型玻璃遮板也可使用，这种遮板附在头盔上可以保护眼睛。这些面罩由厚厚的聚碳酸酯制成，与制造防弹玻璃所用的材质相同。

[image]

返回 - 选头盔的方法：[image]头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

防弹盾牌

值得一提的是防弹盾牌：旨在保护使用者免受枪击的盾牌。

大多数防弹盾牌的防护等级为IIIA级，用于手枪防护，或IV级，用于步枪防护。它们的重量从15到40磅不等。用普通盾牌的方式来挥舞它们是非常困难的。

虽然它们是警察的常用装备，但是它们一般不被军队或民兵使用，也不普遍适用于自卫或社区防卫情况。它们似乎主要用于突袭建筑物。

[image] 防弹盾牌。如果您看到警察举着这玩意，您需要认识它的防御级别

关于防割伤的说明

防割手套和袖套是可以买到的，而且价格也很便宜，但它们一般是为商业厨房中偶然接触到锋利刀具而设计的。这些手套和袖套一般由芳纶（凯芙拉）或超高分子量聚乙烯（Dyneema）织物制成，但有些也含有编织的金属丝。

能抗切割并不意味着能抗刺伤。真正的抗切割袖套对于防御刀子的攻击是有用的，但我们所看到的测试并没有让我们相信目前的产品对于坚决的攻击者而不是工作场所的事故会有很大的帮助。

在美国，抗切割性是由ANSI标准的评分标准来衡量的，从A1到A9，而在欧盟，则是由CE/EN标准的评分标准来衡量的，从A-F（以前是1–5）。ANSI标准的抗切割性比CE/EN标准更高。

[image]

[image]
[image]

您需要真正的自己人-如何组成一个亲密团队：街头实战指南S05E09

[image] 关键词	互助 亲密团队 人际安全 关系 准备工作 团体 安全文化 直接行动
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年1月12日
[image] **Description**	行动安全性

组织是一门科学，行动是技能和智慧的综合爆发，协作是最好的武器，当每个人都能明白这个道理时，我们才有TheNextStep。

- Table of Contents

亲密团队是什么、不是什么
1、亲密团队不是酒肉朋友
2、亲密团队不是圈子
3、亲密团队更像是一支乐队
亲密团队是强大的
亲密团队完全可以是一种灵活的模式
挑选 适合自己的 标准
互相深入了解
决定对您来说适当的安全级别
一起做决定
存在于一个更大的整体中
与其他亲密团队一起组织
底线

2、 行动起来

[image]
[image]

您需要真正的自己人 —— 亲密团队，不论发生什么，都能站在一起共同战斗的队友。尤其是，协调性和对彼此的了解让你们可以很默契地行动。

亲密团队是什么、不是什么

1、亲密团队不是酒肉朋友

—— 酒肉朋友是只能用来享乐的，而很难期待共患难。

酒肉朋友总是想要从对方身上获得些什么，期待给予。虽然酒肉朋友之间也可能有一些共识，甚至有共同的奋斗目标，但能确保他们协调一致地行动的唯一依赖项是，每个人都能明确地有所得。

这在直接行动中是难以保证的和不现实的，行动中唯一可确定的就是风险，包括收益在内的一切都是不确定的；在这种情况下团队需要的是奉献和彼此保护的积极，而不是索取。只有亲密的感情能做到这点。

[image]

返回：[image]如何选战友

2、亲密团队不是圈子

—— 也许圈子会让您想到紧密、内部默契、协调性、共同嗜好和一定程度上的共识等特征，这些基础条件似乎有可能形成亲密团队，但这

两者的组织结构是完全不同的。

由于在圈子中，人们以排斥圈外人为主要凝聚内部的手段，于是圈子是封闭的和不自由的；圈子经常有一个或多个 “领导者”，有明确的或不言自明的等级制度，大多数成员都需要围绕圈子的 “中心” 行事，独立思考将被边缘化甚至被排斥。这在亲密团队中是不会发生的。

[image]

亲密团队必需组合自由，绝不会依靠排外来促进凝聚力，凝聚力来自精神、信念和彼此的爱；没有领导者，或者说每个人都是领导者，这样才能真正充分发挥每个人的潜力、灵活的机动性和创造力。

这是反抗行动者相比官僚主义和等级森严的镇压部队所拥有的 绝对优势 。

3、亲密团队更像是一支乐队

—— 成员不需要追求在各方面保持一致，只需要在具体的行动意向上具有强烈的共识（完成这支曲子的演奏）。

他们彼此了解各自的优势和劣势，知道自己可以从对方身上获得什么、以及自己可以提供给对方什么；他们各自有自己的角色，知道自己的权限，尤其是知道自己如何和队友协作才能完成任务。

[image]

下面具体解释。

不论您想要采取哪种行动，重要的第一步是要先组织起来。单枪匹马是无法成功的。

但“组织起来”并不意味着加入一个已有的机构，接受命令；它不应该意味着放弃您自己的智慧成为另一台机器上的一个齿轮。从行动者的角度来看，组织结构应该最大限度地提高自由和自愿协调的程度，从

最小的群体到整个社会的规模。

您和您的朋友们已经构成了一个亲密团队，是这个模式的基本构件。亲密团队是一个小型的密切的朋友关系网络，每个人把自己理解为一种自主的政治力量。这个想法是，已经相互了解和信任的人应该一起工作，对新出现的情况做出及时的、明智的和灵活的反应。

这种无领导的形式已被证明对各种游击活动有效，也对兰德公司所说的 “蜂群” 战术有效，在这种战术中，许多不可预测的自治团体压倒了一个集中的强大对手。

你们中所有人都应该带着对自己的目标和能力的认识，以亲密团队的形式去参加每一次行动。如果您在一个具有共同行动经验的亲密团队中，您就会有更好的准备以应对紧急情况，并充分利用意想不到的机会。

亲密团队是强大的

它的规模可能很小，但是亲密团队可以产生不成比例的强大影响。

[image]

与传统的自上而下的结构不同，亲密团队可以自由地适应任何情况，它们不需要通过复杂的批准程序来做出决定，所有参与者都可以立即行动和作出反应，而不需要等待命令—— 尤其是，每个人都清楚地知道彼此的期望。

亲密团队所建立的相互钦佩和鼓舞，使他们很难士气低落。与资本主义、法西斯主义的结构形成鲜明对比的是，亲密团队的运作不需要任何等级制度或胁迫。参加亲密团队可以让人感到充实和乐趣，也可以体验到切实的成效。

最重要的是，亲密团队的动机是共同的愿望和忠诚，绝对不是利益、责任、或任何其他补偿性的或抽象的东西。整支防暴警察小队都能被

高度协调性行动的亲密团队所阻挡。

亲密团队完全可以是一种灵活的模式

一些亲密团队是正式的、沉浸式的：所有参与者就生活在一起，分享一切共同的东西，并且这还是一种治疗虚无主义和绝望的方法 —— 爱让它沁过的每个人都充满勇气和力量。

[image]

返回：

返回：https://iyouport.substack.com/p/-4

但亲密团队并不一定必需是一种永久性的安排。它可以作为一个方便的结构，在特定项目期间把感兴趣的和值得信赖的人组合起来。不过请记得，如果您担心被谴责为中文里所描述的 “用人朝前”，您需要努力调整您的组织措施。

一个特定的团队可以作为一个亲密团队不断地在一起行动，但其成员也可以分成更小的亲密团队，参加其他团队的行动，或在亲密团队结构之外行动 —— 这并不是分化！这与分化有着天壤之别；分化是不可逆的，从心态上表现，而自由组织的亲密团队是随时可逆的，一切以任务为中心。

[image]

按照每个人认为合适的方式自由结社和组织，是行动的基本原则；这促进了冗余，因此没有哪个人或哪团体对整体的运作至关重要 —— 否则就会很被动，也给了你们的对手一个重点打击目标的提示，因为你们在各方面只有一个 “要害部位”。

不同的团体应该可以根据需要进行灵活的重组；每个重要部位都应该有替补队员，而亲密团队之外的其他人不应该知道替补者和队友的角色分配。

[image] 亲密团队是一种灵活的模式

挑选 适合自己的 标准

根据您的行动目标，一个亲密团队的人数可以从两个人到十五个人不等。然而，任何团队的人数都不应该太多，您必需能够确保随时可以就紧迫的问题进行非正式的交谈 —— 人太多就不容易召集对话了。

如果需要的话，您可以随时分成两个或多个小组，就像我们在S01教程中介绍的游戏和练习题所体现的那种团队结构。

比如，在需要驾驶的行动中，最简单的制度往往是每辆车上都有一个亲密团队，也就是说，在遇到突发状况时，一辆车上的人们可以不假思索地展开协调性行动。因为他们的协调已经很熟练了。

[image]

返回：[image]S01E02-T1 团队会议安全议题模版

互相深入了解

在组建亲密团队时，首先要了解对方的长处、弱点和背景，这样您就知道您可以依靠对方什么、可以提供给他人什么。

讨论你们对所进入的每一种情境的分析，以及在其中值得完成的事 —— 确定您的队友在哪些方面一致，在哪些方面相得益彰，以及在哪些方面存在差异，这样你们就能在瞬间做出决定。

[image]

培养政治亲密感的方法之一是一起阅读和讨论文本，但没有什么比实地经验更重要的了。

开始的时候要慢慢来，这样才不会过度扩张。一旦你们建立了共同的语言和健康的内部动力，你们就可以确定想要实现的目标，准备一个计划，并付诸行动。

决定对您来说适当的安全级别

[image]

亲密团队能够抵御 渗透者 ，因为所有成员之间都有共同的基本历史和亲密关系，不需要向团体外的任何人通报他们的计划或活动。每个人都了解并能够熟练执行安全文化这是最重要的。

亲密团队一旦组建起来，就应该建立一套共享的安全文化实践，并坚持实践下去。在某些情况下，您可以对您的活动公开透明；而在其他情况下，无论在团队内部发生了什么，都不应该在团体之外谈论，即使所有的活动早已完成。

在某些情况下，除了亲密团队的参与者之外，任何人都不应该知道这个亲密团队的存在。您和您的队友们可以讨论和准备行动，而不向外人承认你们构成了一个亲密团队。

记住，从高安全协议到低安全协议的过渡、比从低安全协议到高安全协议更容易。

一起做决定

亲密团队一般通过协商一致的决策来运作：根据每个参与者的需要和愿望集体做出决定。

在民主投票中，多数人各得其所，少数人必须保持沉默，这对亲密团队来说是非常可怕的，因为如果一个团队要在压力下顺利运作并保持团结，就必须让每个参与者都满意。

在采取任何行动之前，团队的所有成员应该一起确定他们的个人目标和集体目标是什么，他们愿意承担什么风险，以及他们对彼此的期望是什么。这些事项确定后，这个团队就可以制定一个计划了。

由于行动中的具体情况总是无法预测的，计划也很少能如期而至，因此，采用双管齐下的方法来准备可能会有帮助。

一方面，您可以针对不同的情况制定计划。如果A发生了，我们将通过X手段通知彼此，然后转为B计划；如果X手段无法及时联络彼此，我们将在Q时间在Z地点重新召开会议。

另一方面，您可以设置一些结构，即使发生的情况与您想象的任何情况都不一样，也会有用。这可能意味着准备资源（如横幅、医疗用品、或进攻设备），划分内部角色（如侦察、通信、医疗、媒体联络等），建立通信系统（如一次性电话或可以喊出的暗语，以安全地传递信息），准备一般战略（如在混乱的环境中保持彼此的视线），绘制紧急逃生路线，或准备法律支持，以防有人被捕。

行动结束后，一个精明的亲密团队将举行会议—— 必要时，在一个没有任何电子设备存在的安全地点—— 讨论哪些方面进展顺利，哪些方面可以做得更好，以及下一步的工作。

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

[image] 在混乱的抗议环境中，紧密联系的亲密团队采取的行动更加安全。

存在于一个更大的整体中

亲密团队只对自己负责，这是它的优势之一。

亲密团队不受其他组织的程序性协议的约束，没有与陌生人达成协议

的困难，也不受向没有直接参与行动的机构作出答复的限制。

同时，正如一个亲密团队的成员彼此之间努力达成共识一样，每个亲密团队也应该努力与其他个人和团队建立一种类似的体贴关系——或者至少是补充别人的方法，即使别人不承认这种贡献的价值。

理想的情况是，大多数人应该对您的亲密团队的参与或对某一情况的干预感到高兴，而不是怨恨或害怕你们。他们应该认识到亲密团队模式的价值，因此在看到它的成功并从中受益后，自己也会采用这种方法—— 这是需要也只能有您和您的队友做到的。

与其他亲密团队一起组织

一个亲密团队可以与其他亲密团队一起工作，有时被称为集群。集群的形成使更多的人能够以单个亲密团队所具有的同样优势采取行动。

如果要求速度或安全，每个团队的代表可以提前开会，而不是所有团队的所有成员；如果协调是最重要的，各团队或代表可以安排一些方式，通过行动的热度进行沟通。

经过多年的合作，不同的亲密团队可以像了解自己的队友一样了解彼此，相应地在一起变得更加自如和有能力。

[image]

当多个亲密团队的集群需要协调特别大规模的行动时—— 例如，在一次大规模的示威游行之前，他们可以举行一次发言人聚会，在会议上，不同的亲密团队和集群可以相互告知自己的意图（不管明智程度如何）。

这样的聚会很少能产生无缝的一致意见，但是，它可以让参与者了解各种不同的愿望和观点。权力下放所带来的独立性和自发性通常是我们与装备更精良的对手/镇压者作战时的最大优势。

底线

为了使基于共识和合作的亲密团队和更大的结构发挥作用，每个参与的人都必须能够相互信赖，履行承诺。

当计划达成一致后，团队中的每个人和集群中的每个团队都应选择计划编制和执行中的一个或多个关键环节，并提出为其底线。

对资源的供应或项目的完成设置底线，也就是说要保证无论如何都能以某种方式完成的程度。如果您在示威期间负责为您的团队成员管理法律热线，您就有义务确保即使您自己生病了/受伤了/出了什么意外，也有人能处理这项工作，不会误事；如果您的团队承诺为一次行动提供横幅标语，您就有义务确保它们已经准备好了，即使这意味着前一天晚上要熬夜干通宵。答应下的事就必须做到，不论怎么去做。“确保做到” 的程度—— 就是底线。

随着时间的推移，您将会学会如何处理危机，以及在危机中您可以依靠谁 —— 就像其他人会了解他们可以依靠您的程度一样。

行动起来

[image]

不要再想会发生什么，或者为啥什么都没有发生。您需要和朋友们聚在一起，开始自己决定会发生什么。离开被动的旁观者模式，不要再等待别人告诉您该怎么做。

养成讨论您自己希望看到什么发生的习惯，并学习保持信心将这些想法变成现实。

如果没有一个鼓励想法流向行动的结构，如果没有能够一起集思广益、蓄势待发的队友，您很可能会陷入瘫痪，与自己的大部分潜能隔绝；而有了亲密队友，您的潜能可以成百倍、万倍地增长。

人类学家玛格丽特·米德写道："永远不要怀疑，一小群有思想、有决心的人可以改变世界，这是唯一的可能性"。不管她是否知道，她指的正是亲密团队。如果每一个反对国家和现状的行动中的每个人都作为一个紧密联系的、专门的亲密团队的一部分参与进来，革命将在短短几年内完成。

亲密团队可以是一个缝纫爱好者小组，也可以是一个自行车维修小队；可以是为了给占领区为活动家提供一顿饭的厨师小组，也可以是为了通过精心策划的行动计划迫使一家跨国巨头公司破产。

亲密团队种植和保卫社区的花园，建造和占领建筑物，组织邻里托儿计划和野猫罢工；个别亲密团队经常在视觉艺术和流行音乐领域发起革命。

您最喜欢的乐队就是一个亲密团队。

[image]

让五个人相遇，他们将迸发决心行动的闪电而不是生存的痛苦

—— 从那一刻起，绝望结束，战术开始。

[image]
[image]

了解防暴弹药，以及如何保护自己：示威参与者指南S05E10

[image] 关键词	免追踪 直接行动 街头 街头战术 逃亡 防暴武器 防身
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年1月13日
[image] **Description**	行动安全性

在全世界，恐吓都是为统治阶级服务的雇佣军的主要武器。

- Table of Contents
关于标准化和监督
冲击性弹药
常见损伤
保护
了解弹道学
防暴子弹
橡胶球
豆袋弹
橡皮子弹
弹丸和漆弹
路障弹
发射器
.68口径空气动力喷枪
FN303
胡椒球**VKS**
胡椒弹：**280–350 fps**，**12–15**焦耳，**20**米精度，**50**米以上区域饱和度：

VXR弹：280–425 fps，12–28焦耳，50米精度，130米以上区域饱和度：
12口径霰弹枪
37毫米和40毫米发射器
霰弹和榴弹
喷雾器和雾化器
蜡烛
化学武器
战术上的考虑
简而言之就是：
扔回催泪瓦斯罐
中和催泪瓦斯罐
化学武器的作用
给那些特别容易受到伤害的人
免疫力
如何治疗化学制剂的影响
催泪瓦斯和COVID-19
去污湿巾
其他补救措施
日内瓦议定书
化学制剂的种类
1、CS毒气
2、CN毒气
3、CR毒气
4、DM毒气
5、胡椒喷雾：OC
6、PAVA
7、MPK
8、烟雾弹
9、闪光弹
收集废旧弹药
标记
已经能够确定至少有七种警察给人做标记的手段：
去除印记
DNA标记
去除DNA标记
SelectaDNA

[image]

除了用警棍打人之外，镇压者最喜欢干的事就是向抗议的人群发射钝器和化学武器。武器制造商不断开发新的方法来远距离攻击人们 —— 而纳税人不断为他们的压迫者购买新的玩具。

本集内容旨在提供对低致命性镇压武器的概述 —— 包括化学武器和冲击弹药。警察自己也不屑于区分这两种武器。

我们将介绍化学武器，如催泪瓦斯和胡椒喷雾；也将介绍冲击性武器，如防暴子弹、橡皮子弹和胡椒球。

我们将介绍警方使用这些武器的系统，包括气枪、喷雾、榴弹，榴弹发射器、和猎枪。

还将介绍警察在逮捕抗议者时做标记的方式—— 以及他们可能不做标记的方式。

[image]

返回：[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06

[image]

这可能是一个可怕的主题。但请记住 —— 镇压者的目的不是用塑料子弹打我们，也不是用化学品喷我们；他们的真正目的是让我们生活在恐惧中，他们希望我们呆在家里，与世隔绝，让他们的权威绝对化、永久化、不受挑战。

每次我们一起上街，当权者都无法实现他们的目标。

每次我们拒绝让恐惧支配我们的行为时，当权者都会失败。

（以下视频是缅甸抗议者最近对盾牌用法的演示）

https://vimeo.com/554571375?fl=pl&fe=sh

本集内容将简单地触及如何通过防毒面具、盔甲、盾牌等防护工具来保护自己，前面几集的内容已经详细探讨这些选择。但最能保护我们免受警察侵害的最重要工具是：团结。我们彼此是必须保护对方安全的人。

示威前线的一个盾牌可以保护很多人；一个愿意在火线救治的医护人员，可以保护很多人；几个亲密团队的伙伴冒着坐牢的危险把警察逼退，可以保护更多人……

[image]

我们对付防暴弹药最好的保护方法就是我们彼此之间的爱。

勇气不是没有恐惧；而是在恐惧的情况下采取正确的行动。团结起来，我们就能克服恐惧。

[image]
https://x.com/bishonentype/status/1344917667551952896
https://x.com/bishonentype/status/1344917667551952896

关于标准化和监督

没有发现任何证据表明政府对警察获准使用何种武器平息内乱有任何监督。据一位专门从事这一领域工作的律师说，比如在美国，大约18,000个机构中的每一个机构都有自己的使用武力准则，详细规定了关于其官员可以对老百姓做什么的内部标准。也就是说，它并没有一个统一的可查的标准。

没有发现任何机构认证化学武器中使用的化学成分是什么；任何特定的化学武器制造商都会选择他们自己的结合剂和化学添加剂；似乎没有一个简单的方法可以知道当警察使用这些武器瞄准我们时，我们接触到的究竟是什么化学品。网络上常见的抵制化学武器的那些参考资料也许并不实用。

虽然这不应该让我们退缩和屈服于专制主义，但重要的是要记住，这

些武器与实弹相比，只是“杀伤力较小”。

[image]

但规律还是有一点的。

促使这些武器标准化的因素只有两个。

第一是使用现有弹射系统的武器（如37毫米发射器）比需要全新训练和武器装备的奇葩系统更容易被广泛采用；二是制造商往往会互相模仿创新。

虽然政府显然没有提供监督，但它偶尔也会提供意见和建议 —— 例如，2004年这本有些过时的低致命性武器手册。

冲击性弹药

警察用各种武器发射各种钝力弹。制造商和警察部门有时将这些弹丸称为“钝力冲击弹” (BIPs) 或“动能冲击弹” (KIPs)。“橡皮子弹”只是众多变种中的一种，它们的大小、威力、成分、发射方式和杀伤力各不相同。

制造商向镇压机构进行的推销强调了通过发射获得令受试者服从的能力，而伤害或死亡的风险最小。所有的学术研究 —— 更不用说我们的亲身经历了—— 都表明，这两种说法都不正确：反冲锋弹药经常使抗议者致残或死亡，而且它们很少能成功地驱散示威活动。它们在阻止社会运动方面的效果更差；通常情况下，当我们中的一个人失去一只眼睛或头骨骨折时，更多的人就会走上街头。

一些比较常见的冲击性弹药包括：

- 防暴子弹，塑料、泡沫、凝胶甚至木质弹丸，由多管发射器发射，偶尔也有用猎枪发射的；

- 橡皮弹子、涂有橡胶或PVC的金属弹丸；
- 豆袋弹，装满二氧化硅或铅珠的编织袋，通常由猎枪发射；
- 胡椒球，本质上是装满胡椒喷雾的漆弹；
- **FN303**弹，是胡椒球和普通冲击性弹药的组合；
- 橡胶球，橡胶或塑料或泡沫颗粒，装入榴弹中，它们会像弹片或枪弹一样爆炸；当然还有老式的毒气罐 (带有化学制剂或烟雾)，理论上它不是用来直接向抗议者发射的，但镇压者经常这样做。

与流行的说法相反，大多数现代冲击性弹药是为 “直射” 而不是 ”跳射” 而设计的；直射弹药是为了直接射杀个人，而跳射弹则是为了在地面弹跳从而进入人群。

催泪弹罐一般用于近距离的跳射或向空中以25–30度的弧度发射，以获得最大的射程；它们的额定值不应该被用于直射。

有些样式的警用防暴子弹分裂成多个弹丸，是为了以跳射方式设计的，以使弹丸分布更广，而另一些则是为了在抗议者的头顶上发射，以便将化学制剂洒下来。

全尺寸的木制防暴子弹和一些橡胶子弹似乎也是为跳射设计的，但总的来说，跳射的准确性较低，也不常见。

[image]

防暴子弹、橡皮榴弹和豆袋弹都会伤人，偶尔，它们会使人致残或—— 直接使人死亡。然而，在警察使用的所有镇压工具中，它们是最不能有效阻止示威的一些工具。防暴子弹不能逮捕你；它也不像一团毒气那样迫使人群驱散。

射程冲击性武器主要依靠制造疼痛而强迫顺从。虽然这可能对个人有效，但仅靠疼痛通常无法迫使坚决的人群服从。冲击性弹药的影响可以通过防护装备来减轻，包括盾牌、盔甲、头盔、护目镜、路障，甚至雨伞。

冲击性武器的有效性首先依靠的是人的恐惧，而通过心理准备和相互支持，我们就可以抵御恐惧。我们可以选择拒绝顺从于恐惧。

[image] 在全世界，恐吓都是为统治阶级服务的雇佣军的主要武器。

常见损伤

冲击性弹药表面上是为了伤人，强迫人们屈从而不造成重大伤害。但是，它们的实际杀伤力比人们想象中的大得多。

现有数据非常多，最大的研究来自2017年，包括来自世界各地许多其他研究的信息。但其数据中的很大一部分 —— 约41%—— 描述了橡皮子弹的使用情况。在研究中，橡皮子弹在严重伤害中占据了绝大比例，在死亡人数中也占了稍大的比例。研究发现，在遭受冲击性弹药受伤的人中，有3%的人因此而死亡。

2017年的研究发现，大部分重伤和死亡是头部或颈部受到冲击的结果。2000年的一项规模较小的研究发现，大多数死亡是撞击胸部的结果（导致肋骨断裂，刺穿心脏或肺部）。

除发射的弹药类型外，决定伤害严重程度的最重要因素是发射的距离和受害者获得医疗救助的速度。例如，10英尺以内的攻击造成的骨折最多。另外，街头医护人员也能挽救生命。

冲击性武器最常见的伤害是强烈的瘀伤。而尽管警察缺乏能力，行为不受惩罚，但似乎大多数冲击性弹药确实瞄准了它们应该瞄准的地方，腹部或下部，那里不太可能发生严重伤害。

偶尔也会有镇压部队直接向人的身体发射旨在突破门等障碍的弹丸，

大概是不小心发射的，那样就会发生伤亡。

乔治·弗洛伊德起义三周后，美国眼科学会报告说，在抗议活动中，至少有**20**起严重的眼伤是由冲击性武器**——** 包括防暴子弹、豆袋弹和胡椒球、以及催泪弹**——** 造成的，其中有一起是由泰瑟枪造成的。其中包括**7**次有人因这种事件而失去眼睛的情况，是的，瞎了；还有很多人在等待手术，不知道是否能保住眼睛。在今年的一起案件中，一名记者因一枚弹丸打破了他的防毒面具的保护镜片，导致眼睛严重受伤。

世界各地的医学专家一直在并继续呼吁在警务工作中废除冲击性弹药。

[image] 在今年的美国反抗运动中活动家制作的呼吸器简介

保护

根据街头经验和研究分析，最需要保护的部位是头部、眼睛、脖子和胸部。
gorget、运动装甲胸甲以及防撞镜、面罩或防毒面具都可以起到保护作用，有
与盾牌相结合。颈部是这些部位中最复杂的保护部位，大多数人从来没有听
“gorget” 这个词，更不用说想象在抗议警察的时候戴上一个了。基本上，gor
是击剑手佩戴的一种颈部盔甲。目前还没见过有人在示威活动中戴着它。

【注：gorget 是用于保护喉咙的钢或皮革项圈，一组板甲或从颈部垂下并覆盖喉咙和胸部的单片板甲。后来，特别是从18世纪开始，它成为军服的象征性配饰，这种用法在一些军队中得以幸存。】

我们将在以后的文章中详细讨论盾牌。在这里只想说，为了抵御冲击性弹药，盾牌必须足够坚固，能够抵御子弹的穿透，足够坚硬，能够将冲击力分布在大面积的表面，并且在持盾者身体接触到的地方有泡沫支撑。3/8” 厚的胶合板就足够了，不过1/2” 可以承受更多的冲击性武器。交通锤塑料能很好地抵抗穿透力，但力量分布不均，不过它比木头轻得多。请记住，没有哪种盾牌能让您坚不可摧。

大多数伤害发生在腰部以下。经验上看，训练有素的警察更喜欢射杀示威者的膝盖骨。有鉴于此，可能值得考虑穿戴护膝或更完整的运动装甲，与其说是为了避免永久性伤残或死亡，不如说是为了保持机动性、有效和不受伤。

盾牌和路障也可以帮助减轻所有这些潜在的伤害。

[image]

了解弹道学

要了解冲击力，我们必须先了解动能。

动能，在弹道学中常被称为枪口能，以焦耳（或以英尺-磅为单位）来衡量。它是由物体的速度和它的重量推导出来的，速度的重要性是指数级的。确定弹丸动能的公式是 Ek = (1/2)mv2，Ek代表能量（动能），m代表质量，v代表速度。

我们都不是工程师，但在写这篇文章的过程中，我们咨询了几个人。基本上可以理解为焦耳用来衡量
“我被击中了多少” 这个问题的答案。一个以90英里/小时的速度扔出的棒球可能有120焦耳；一发警用防暴子弹可能有240焦耳，于是它击中您的力度是棒球的两倍。一支点22步枪可能也会发出240焦耳的弹丸，但警用防暴弹是一种钝性冲击，而步枪子弹是为了穿透。9毫米手枪可能发射470焦耳的子弹，AR-15的子弹是1850焦耳，而12毫米口径猎枪的弹头可能接近4500焦耳。如果一个180磅重的人从15英尺高的地方摔下来，他落地时大约有4000焦耳。一辆飞驰的汽车呢？大约20万焦耳。

然而，我们大多数人宁愿被防暴子弹击中，也不愿被.22口径的子弹击中。但焦耳远不是一个特定弹丸所能造成的伤害的全部。它击中您的表面积 (每平方米的焦耳数)、击中您的角度、击中您的身体位置、以及物体的成分 (例如，木制的防暴子弹比胶质防暴子弹吸收的自身冲击力要小) 都更重要。在一项研究中，当以一定角度施压时，只需要375焦耳就能将骨头打碎，而以其他角度施压时，打碎同样的骨头

需要9920焦耳。

由于速度对能量的影响比弹丸的重量更重要，所以弹丸击中目标的能量在距离上会迅速下降。速度较快的物体往往比速度较慢、重量较大的物体携带更多的动能。

从各种武器所能提供的能量以及各种防护装备所要接受的冲击测试开始，是很有用的。我们发现有一份军事文件提到75焦耳的 “国际公认杀伤力限度” 。但这些因素并没有给我们提供足够的信息以了解特定的弹丸会对特定的目标产生怎样的影响。在针对各种防护装备测试各种冲击弹药的同时，希望听到您能够分享的关于不同形式的射弹防护效果的任何轶事或研究。

防暴子弹

- 材料构成：塑料、泡沫、凝胶、木头

- 发射方式：主要是37/40毫米发射器，一些12毫米口径猎枪

- 速度：大多数似乎在 300fps（每秒英尺）左右，有些例子高达650 fps

- 能量：一个例子是244焦耳

- 射程：取决于广泛的构成，但总体宣传的射程在1.5米至80米之间

防暴子弹有多种形状、大小和材质，但它们基本上是大块的物体以制造痛苦。它们往往是大口径的 (37毫米和40毫米)，这样它们就能产生尽可能大的威力，同时又不会穿透皮肤。许多防暴子弹还包括某种有效载荷，如化学剂或标记染料。

大多数被称为 “橡皮子弹” 的弹丸可能都是防暴子弹。没有必要迂腐地纠正人们的观点，但为了本文的目的，我们要做出区分，并将其称为防暴子弹。

防暴子弹最常见的材料是塑料、泡沫、凝胶和木头。虽然品种太多，不一一列举，而且不同的厂家使用不同的材料用于不同的用途，但总体看来，泡沫弹往往是用于短距离射击的，而塑料和木头则是用于长距离射击的。凝胶弹和 “可压缩头” 的塑料弹一样，都被宣传为在短距离或长距离上有用。当然，很难想象镇压部队真的会想清楚到底要用哪种子弹来达到哪种战术目的，尤其是在混乱的情况下，可以肯定的是，他们在任何范围内都会发射这些子弹。他们手头有什么就会发射什么。

[image] 40毫米泡沫防暴子弹

防暴子弹通常在每个弹壳内装有多个弹丸，这些弹丸被设计成可以分裂。

有些防暴子弹在弹体或发射器的枪管内有膛线，以使弹丸自旋稳定，从而提高精确度。多数似乎没有。虽然每种防暴子弹的额定射程不同，但大多数似乎是为2至40米之间的使用而设计的；只有少数品种的设计射程可达80米。

直射的防暴弹理论上应该是瞄准人的肚脐、大腿、臀部或膝盖 —— 虽然如前所述，期望警察以此为限绝对是个错误。

大多数被防暴子弹击中的人只是留下了一个恶心的伤口，然而防暴子弹致残和致死的情况也时有发生，特别是当它们击中人的脸部时。7月，波特兰警方用防暴子弹射中了一名26岁的抗议者的脸部，而当时他的手是举着的。我们认为那发子弹是 Sage International 37毫米KO1子弹。这一击使他的头骨骨折，几乎丧命，必须进行手术。

此外，还有12号猎枪防暴子弹。这些大多是各种橡胶弹丸，它们有翅片，看起来就像小型导弹。例如一个重6克的子弹，要以426 fps的速度发射，总力道为51焦耳。我们发现了一个视频，有人把子弹装错了，结果以三倍的速度射击。并且已经看到一些证据表明，警察在美国的抗议活动中使用了这些武器。

https://youtu.be/0j5x7MTFAEQ

防暴子弹似乎是英国人发明的，用于他们在爱尔兰的殖民项目，因为他们当时使用的橡胶子弹杀伤力太大。塑料防暴子弹仍然会杀害殖民对象，但速度较慢。

现代的防暴子弹往往含有一种或多种化学武器，其中最常见的是OC（胡椒喷雾）和CS（普通催泪弹物质），不过CN（更危险）也被使用。有些防暴子弹还含有标记化合物，就是射中身上很难洗掉，以此来在事后追踪抗议者的身份。

[image] 37毫米木质防暴子弹

橡胶球

- 构成：硬橡胶
- 发射工具：榴弹发射器、37/40毫米霰弹筒、12口径猎枪，可能是.68口径的气枪
- 速度：可变
- 能量：用猎枪发射时为30–200焦耳，其他样式不详。
- 范围：变化较大

橡胶球有些是单独发射的，或者更多的时候是装在猎枪弹、多管火箭弹、或榴弹中。它们发射出来的子弹很疯狂，伤人程度难以预料。品牌名称包括 “毒刺”（Stinger）、“刺球”（Sting-ball）和 “马蜂窝”（Hornet’s Nest）；它们有时被笼统地描述为橡胶弹。

我们发现了几种常见的橡胶球的口径：.32口径和 .60口径（也就是 .32” 和 .60″），在榴弹和较大的弹罐中很常见，而橡胶弹似乎有 .33″。有些霰弹枪的子弹里装着1到3个.68” 的橡胶球。

[image]

根据一家制造商的说法，橡胶球武器被认为是在其他杀伤力较小的选择失败时的最后手段。这可能是因为橡胶球在攻击谁和在哪里攻击都是不可预测的。

有可能，虽然我们还无法确认，但在美国，人们所说的橡胶弹大多是口径较大的橡胶球。组合战术系统在波特兰市很常见 —— 据推测，8月份警察就是用这种手段打断了某个抗议者的手指。据传闻，很多橡胶球似乎都会走火，因为示威者发现了大量部署不当的弹筒。

[image] 一个橡胶球榴弹

据推测，过期的橡胶球随着时间的推移会失去一些弹性，变得更加危险。

橡胶球也被装入手榴弹中，就所有其他用途而言，它的功能是闪光爆炸式榴弹那种：利用声音和光来分散人们的注意力的迷惑性装置。我们看过的一款榴弹，ALS马蜂窝刺痛榴弹，可以装180个.32口径的球，在5英尺处产生1–2万坎德拉的闪光和130分贝的爆炸声。

[image]

橡胶球的移动非常混乱，在地上引爆的榴弹很容易将弹丸射向抗议者的脸和眼睛。

这些榴弹绝对不安全，不应接住或扔回去。

[image] 12口径橡胶弹

豆袋弹

- 组成：硅或铅在凯芙拉或其他织物中包裹的弹丸

- 发射方式：大多数是12毫米口径猎枪，但也有37/40毫米发射器

- 范围：20–35英尺
- 速度：大约270 fps
- 能量：一个12口径的例子是146焦耳

豆袋弹是装满金属或二氧化硅的袋子。平均来说，它们比防暴子弹的使用距离更近；它们更经常用于建筑物内射击 —— 特别是监狱内。每个制造商和每一发子弹都会有所不同，但大多数似乎是为了在20–35英尺之间使用。有些豆袋弹是 “拖动稳定” 的，以保持其整个有效距离内的准确性。它们由37毫米和40毫米发射器和12口径猎枪发射。

制造商的指南表明，使用豆袋弹需要2–3次射击才能使目标丧失行动能力。在混乱的情况下使用它们时，通常不是为了使人丧失能力，而是为了给人群造成心理冲击。

在论坛上看到一位警察讲述了一个人服用PCP后，在34发豆袋弹中幸存下来的故事（虽然有一发子弹打碎了他手上的骨头）。网络论坛上的警察经常吹嘘自己如何用豆袋弹射杀菜鸟，让他们晕头转向。

【注：PCP是苯环利定或苯基环己基哌啶，也叫天使尘，是一种因其改变思维的作用而使用的药物。PCP可能导致幻觉，声音感知失真和暴力行为。是一种娱乐性毒品】

[image] 40毫米豆袋弹

橡皮子弹

- 构成：橡胶或尼龙或PVC涂层的钢、或橡胶和二氧化硅的硬性物质构成

- 发射方式：多种多样

迄今为止，我们对橡皮子弹的研究不如对其他子弹的研究更有定论。从历史上看，用于控制人群的橡胶弹有两种形式：一种是涂有橡胶的金属弹丸，如英国占领者在北爱尔兰广泛使用的那种；另一种是由大约**20%**的橡胶和**80%**的二氧化硅的混合物制成的硬弹丸，如以色列占领者在巴勒斯坦普遍部署的那种。

美国的警察是用橡胶球来射杀人的，有人猜测**2020**年华盛顿特区的警察已经使用了多年来害死很多人的钢芯弹种。

由于在2017年对低致命性武器的研究中，金属芯弹丸在致死和致残中占比过高，这值得进一步调查。

还有一些子弹形状的橡胶弹，设计成可以从9毫米手枪和大概其他所有常见枪支口径发射。但由于这些是由普通枪支发射的，所以似乎还没有找到进入警方防暴武器库的途径。到目前为止追踪到的唯一一家制造这种子弹的制造商是在加拿大：**Lamperd Less Lethal**。

[image]

最安全的假设是，您看到的警察携带的步枪和手枪都装有实弹。

弹丸和漆弹

越来越多的致命性较低的弹药是由 0.68” 口径的气枪—— 也就是漆弹枪发射的。

虽然这两种都是作为冲击性弹药使用的，但它们都有各自的发射器，所以我们会在下面的 “发射器” 部分进一步介绍它们。然而，法西斯分子最近已经采用漆弹枪作为街头冲突的有利工具，有很多传言说他们使用的是冷冻漆弹，但我们怀疑他们可能使用的是橡胶球。

冷冻漆弹在漆弹界几乎是个神话，因为当地媒体谎称它们是万圣节破

坏者青睐的工具。漆弹在家用冰柜中冷冻48小时，并不会冻成固体，它们只是变得稍微脆一点，粘性大一点，而且很快就会解冻。而在干冰中冷冻的漆弹则更加坚固，有潜在的危险性，但射击时却很笨重。液氮冷冻的漆弹和冰一样硬，但非常脆，几乎不可能装填和发射。所有的冷冻漆弹都会变得不那么准确——
因为弹壳变得更粘稠—— 但刺激性更强。

在世界上一些地方，由于自卫用的枪支不那么普遍，气枪有时被用来提供近乎致命的力量，发射的弹丸包括固体橡胶或PVC涂层的钢球，如上面橡胶弹下列举的那些，有时被称为 “玻璃破碎机” 球。这些弹丸当然可供警察部队以及平民使用；它们可以从任何漆弹发射器中发射。

[image] “Glass breaker”

Antifa 活动家泄露了2020年在波特兰的极右翼通讯记录，显示至少有一名极右翼民兵讨论了使用冷冻漆弹的问题，但指出其缺乏准确性。他建议改用玻璃破碎球，如上文详述。

还有一些气枪发射的自卫弹，使用像 First Strike 这样的D型弹。First Strike 是一种从弹匣而不是弹斗中发射的漆弹弹种，旨在提高精度。同样的系统已经被改造成可以发射橡胶弹丸，其威力足以致命。

我们没有看到警方使用它们的证据，除了下面胡椒弹栏目下所涉及的 Pepperball VXR 弹，还有FN303弹。

[image] FN303弹

路障弹

路障弹是一种射弹，设计用于穿透玻璃窗(12gauge)、空心门(37毫米) 、或薄墙板或胶合板 (40毫米) 等坚硬的障碍物，并在撞击上述障碍物时释放化学剂。它们在击穿双层窗户或厚重的窗帘方面效果不佳。这些子弹理论上不是用来向人发射的；但它们已经杀死了许多被它们直接击中的人。

它们携带OC、CS、CN、或惰性液体或粉末。携带液体的更重，能更有效地穿透障碍物，而携带粉末的则能更有效地散播毒气。液体子弹带有红色染料，可以标记它们击中的位置。

发射器

警察可以使用各种各样的工具在远距离投射武力。其中最常见的包括.68口径气枪 (实质上是漆弹枪)、12口径猎枪 (被称为并通常被标记为低杀伤力猎枪，但实际上可与任何其他**12**口径猎枪相当)、榴弹和37或40毫米 “多管发射器”，其功能是榴弹发射器。

这些武器尽管制造商有承诺，但并不是特别准确。

研究表明，当低杀伤力武器的操作者处于压力之下时，他们在30米以上的垂直精度会大打折扣。其他因素还包括疲劳、发射器本身的重量（装填时重量很大）和子弹的后坐力。这些细小的差异在距离上的影响会成倍增加。

在近距离内的一英寸差异，在较远的距离内可以变成几英尺的差异。这意味着，即使一名警官选择将这种人群控制武器瞄准某人的下半身，他也可能很容易击中目标的头部或完全击中其他人。没有一种万无一失的方法可以将任何武器射入人群中并确定击中预定目标。

.68口径空气动力喷枪

警察用相当于漆弹枪的东西向人们发射化学剂、冲击弹药和标记弹。这些都是.68口径的空气动力喷枪和手枪。曾经，这些枪几乎只用来向抗议者发射胡椒球和漆弹，但不久之后，有一家制造商在弹丸中加入了冲击性弹药，制造出既含有化学剂又有足够金属伤害力的尾翼稳定射弹。

.68口径的 “低杀伤力” 武器和弹药似乎有两个主要的制造商：

Pepperball 和 FN Herstal。我们将重点以每家的旗舰产品为例，但警方可能会配备这些武器的旧型号、这些武器的手枪版本、或完全来自其他公司的系统。手枪版的 Pepperball 系统似乎比其他选项的精度更低。

[image] 手枪版的 Pepperball

还有大量的 “防暴子弹” 式弹药，设计用于气步枪/漆弹枪发射 (包括0.68口径和0.50口径)，这些可能是任何东西，从固体橡胶球到PVC涂层的钢丸，再到使用 First Strike 漆弹枪以提高精度的D形弹丸。

[image]

有很多关于运动员遭受普通漆弹伤害眼睛的传闻。这些较小的弹丸在抗议活动中可能特别危险。这是一个戴护目镜的好理由。

在美国执法部门已知采用的两种武器系统中，**FN303**在疼痛、伤害和死亡方面似乎大大增加了危险性，而**Pepperball**系统的战术通用性更强。

[image] FN303.

FN303

- 有效范围： 50m
- 范围： 100m
- 口径：0.68
- 弹匣容量：15
- 重量：5磅
- 速度：295–300 fps

- 能量：35焦耳
- 上市价格：1699美元
- 弹药价格：2.85–4.65美元/发（漆弹较便宜，化学武器弹较贵）

FN303是一种利用压缩空气向目标发射子弹的枪。虽然实际枪管很小，像其他漆弹枪和胡椒弹枪一样发射0.68英寸的弹丸，但FN303从某些角度看有点像榴弹发射器，因为压缩空气罐位于枪管上方，可能会被误认为本身枪管较大。

它发射的是聚苯乙烯弹丸，为了保证精度，它的弹丸是经过精细稳定的。每个弹丸的前部装有微小的铋丸，后部装有有效载荷。铋基本上是铅的无毒替代品。前段的设计是为了在不穿透皮肤的情况下提供创伤；但对弹道凝胶的测试表明，无论如何，它经常会穿透皮肤，波特兰的抗议者发现，这种子弹可以穿透自行车头盔。铋弹丸可以穿透皮肤，并在人工取出之前保持嵌入数周。

FN303有10英寸的枪管（比步枪短）和15发鼓形弹匣。气罐可以在需要加注之前发射110发子弹。安全装置在扳机护罩内。整个装置可以从枪托上取下，安装在步枪的枪管下，不过幸运的是，我们还没有看到任何民警这样做的证据。它也有手枪形式，有一个六发弹匣。

每枚FN303弹丸重8.5克。市场上有五个版本，每个版本都有颜色编码。白色弹丸含有惰性火药，用于训练；透明弹丸没有后部有效载荷，仅用于伤人；橙色弹丸含有PAVA火药（合成胡椒喷雾，见下文）；粉色弹丸含有粉色的、水溶性的、可清洗的涂料，用于标记目标；黄色弹丸含有黄色的、乳胶基的、难以清洗的涂料，用于标记目标。这些弹丸在原铝箔包装中保存时，保质期为三年。

2004年，一名波士顿警察用**FN303**枪杀了 **Victoria Snelgrove**。据称，该警员当时瞄准的是人群中的其他人。弹丸进入了 **Snelgrove** 的眼睛，击穿了骨头，伤及大脑。几小时后，她因伤势过重死亡。

研究表明，单个**FN303**在发射几百发子弹后就会失去准确性；FN303是上述研究中使用的武器，表明在紧张的情况下，致命性较低的武器在操作者手中是多么地不准确。波士顿市因此停止了FN303的使用，其他几个城市也是如此。但在写这篇文章时，波特兰警方继续使用FN303，估计全国许多其他部门也是如此。

在卢森堡，**2009**年，首次使用**FN303**的警察开枪打伤了一名记者的手指。

2020年，波特兰警方用**FN303**射杀了一名国家地理杂志的电影制片人；它打破了那位电影制片人的M10防毒面具的塑料镜片，撕裂了他的眼睛，必须进行手术。几周后，仍有铋丸嵌在他的脸部皮肤上，看起来像小黑头，他一直在用针自行清除。

[image] 2020年7月，联邦特工在俄勒冈州波特兰市向与PBS和《国家地理》合作的摄像师 Trip Jennings 开枪。

胡椒球VKS

- 胡椒球的有效射程：20m
- VXR的有效射程：50m
- 口径：.68
- 弹匣容量：弹匣10–15发，弹仓180发。
- 重量：6.2磅（未装填）
- 能量：可在10–28焦耳之间调整
- 速度：280–425 fps

- 上市价格：约1200元

- 弹药价格：未知

Pepperball VKS(可变动能系统) 本质上是一把漆弹枪，其设计外观和功能与AR-15类似，可以发射充满胡椒喷雾或其他子弹的漆弹。用户可以通过旋转枪管，在通过步枪式弹匣（可以装胡椒弹或异形弹）或漆弹式弹斗（只装胡椒弹）给它们供弹之间进行切换。它们还可以使用两种不同的压缩空气源：枪托本身是一个压缩的13ci HPA气罐，或者一个远程气管可以连接到任何压缩空气罐。网上论坛认为从13ci气罐中可以获得多少发子弹的范围很广，估计在80–250之间。AR式安全开关有三种模式：(S)安全, (F)射击, (D)拆卸。速度调节螺丝位于右侧扳机上方。VKS有黑黄、黑橙、全黑三种颜色。制造商的指导说明，该武器不能射向头部、面部、眼睛、耳朵、喉咙或脊柱。

警察部门使用胡椒球进行直接冲击以及区域饱和。丹佛市警察局的一名训练员说，警方使用胡椒球是为了饱和一个本来很危险的区域，吸引嫌疑人从躲藏或掩护中出来。

步枪发射的弹药有两种：圆形胡椒弹，从弹斗或弹匣中装填，精度可达20米；还有一种新式弹药VXR形弹，只能从弹匣中装填。VXR型弹丸由于采用了鳍式稳定，所以精度可达50米。

这种步枪的射弹速度可以达到425fps。相比之下，为了安全起见，大多数漆弹射击场都将枪支限制在280fps以内。

每一发子弹都有颜色编码。弹药的保质期为3年。

[image] 胡椒球发射器

胡椒弹：280–350 fps，12–15焦耳，20米精度，50米以上区域饱和度：

- 白色和红色：LIVE, 0.5%的PAVA(合成胡椒喷雾)

- 黑色和红色：LIVE-X，5% PAVA
- 白色和蓝色：CS，2.5% CS（催泪瓦斯）
- 蓝色和红色：CS/PAVA，1.25% CS和1.25% PAVA
- 白色和紫色：惰性，用于训练或仅仅是为了伤人
- 纯绿色：标记，含有识别用的油漆
- 纯白色/米色：玻璃破碎器，设计用于破碎玻璃，然后自己破碎，不设计用于人或动物
- 无色：充满水，用于训练或只是用来伤人
- 也是无色：紫外线标记，用于用只有在紫外线下才能检测到的墨水给人做标记

VXR弹：280–425 fps，12–28焦耳，50米精度，130米以上区域饱和度：

- 红色和橙红色：VXR Live，0.25% PAVA
- 红色和黑色：VXR Live-X，2.5% PAVA；
- 蓝色和黑色：VXR CS，1.25% CS
- 蓝色和红色：VXR CS/PAVA，0.625% CS粉 和0.625% PAVA粉

- 紫色：VXR惰性粉末，用于训练或仅仅是为了伤人

- 白色和黑色：VXR惰性液体，用于训练；可能含有标记涂料—— 文件不清楚

- 深蓝色和黑色：VXR标记，含有识别用涂料

- 也有白色和黑色两种：VXR紫外线标记，用于只有在紫外线下才能检测到的墨水给人做标记

[image] “低致命性” 霰弹枪

12口径霰弹枪

12口径霰弹枪发射了大量杀伤力较低的射弹。豆袋弹是最常见的，但也有橡皮球弹，还有防暴子弹，以及枪口爆炸弹 —— 一种直接从枪管中散布化学剂的手段，射出10–15英尺左右的尘埃云。

请注意，“防暴霰弹枪” 的名称并不适用于专用的低致命性霰弹枪，而是描述了为防御性战斗而设计的霰弹枪，与用于狩猎的猎枪或用于进攻性战斗的战术霰弹枪不同。

我们没有发现证据表明有任何监督规定警察部门必须使用专用的低致命性霰弹枪，尽管大多数部门都在使用。专用的低杀伤力霰弹枪一般是通过在枪托和/或前端使用明亮的橙色、红色或其他颜色来指定的。虽然有些型号的霰弹枪是专门为低致命性使用而出售的，但许多部门对现有型号进行了改造，以代替颜色代码。这使得它很难提供关于什么款式的枪在被使用的具体细节。

大多数警用霰弹枪都是泵动式，因为这些霰弹枪能够发射更多种类的弹药。半自动霰弹枪通常是利用子弹的反冲力来给下一发炮弹上膛，如果使用不同类型的弹药，这种力道是不规则的，会造成进弹问题和卡壳。

大多数警用霰弹枪的枪管似乎都是14”或18”。一般认为平民拥有14‘’枪管的猎枪是非法的。大多数泵动式霰弹枪可装4至8发子弹。我们发现的一款杀伤力较小的18‘’猎枪可装6＋1枚弹壳：即机匣筒内装6枚弹壳，1枚弹壳上膛。

然而在当地收到的报告说，警察使用全长猎枪，大概枪管长度为26或28”‘。克利夫兰的一位活动家报告说，携带这些猎枪主要是为了恐吓，而同一部门则用18”‘枪管的猎枪发射实际杀伤力较小的子弹。

枪支的枪管越长，精度就越高，弹丸的速度也会越快，冲击力也可能越大。

路障弹可以从12口径猎枪中发射。它们不是为直接向人射击而设计的。尽管如此，由于它们装在致命性较低的霰弹枪中，警察们还是用直接射击杀死了许多人，可能是无意的。

与此相关的是，“破门弹” 是用来破坏锁和门的。这些猎枪弹一般由小金属弹丸或金属粉末组成，通常是铅，悬浮在蜡等介质中。其想法是，子弹在撞击前保持刚性，将能量释放到铰链、锁或门框中，然后在撞击后破碎。

无论是路障弹还是破门弹，伤害都来自于最初的撞击，它可以将致命的能量传递给目标。

几家警用弹药制造商出售 “榴弹发射杯” ，它可以连接到12口径霰弹枪的枪口上，使警察能够发射通常用手投掷的手榴弹。使用时，将榴弹发射杯固定在枪管末端，然后将特殊的发射弹壳装入枪内。

[image] 12口径豆袋弹

37毫米和40毫米发射器

大多数防暴弹药 —— 包括催泪弹、枪口爆炸弹、闪光弹和标记弹 —— 都是由设计成榴弹发射器的装置发射的。为了消除歧义，我们将把它们称为 “多管火箭筒” ，因为它们发射的装置范围很广，不只是榴

弹。这些东西有时也被称为“防暴枪”或“不那么致命的发射器”，但“防暴枪”在美国经常被用来描述真正致命的“防暴霰弹枪”。

常见的多管发射器有两种口径，37毫米和40毫米。传统上，40毫米发射器被视为“军用”，37毫米发射器被视为“民用”，但警方同时采用这两种发射器，两者的区别似乎不大。

在美国，平民拥有37毫米发射器是可以合法的，只要他们使用的弹药不是杀伤性的，信号弹和烟雾弹是合法的，而防暴弹则不合法。还有38毫米弹药，我们看到的大多数37毫米低杀伤力发射器在广告上也是发射38毫米弹药的。**38**毫米弹药在美国以外的地方可能更常见。

抗议场合使用的所有40毫米榴弹似乎都符合北约低速榴弹的“40×46毫米”标准，这也是手持发射器使用的标准，与40×53毫米高速榴弹不同的是，40毫米榴弹一般由挂载式武器发射。这些系统之间的弹药是不能互换的。

许多多管火箭筒的炮弹用的是黑火药，而不是用会产生火花和烟雾的现代火药。这样做是因为这些弹丸比大多数现代弹药更易碎。有些有“无烟”型号，据推测，这些型号使用的是EC无烟火药，这是一种稍为现代的黑火药变种，产生的烟雾较少。

当人们震惊地报告说，在公立学校工作的警察有“榴弹发射器”时，这很可能是指多管发射器。警察可能并不打算向学生发射实弹，而是打算用《日内瓦公约》明确禁止在战争中使用的化学武器毒害学生。

手枪式发射器是存在的，但一般只为枪口爆炸弹设计。

全尺寸的发射器通常是后膛装填的单发枪（枪管与枪柄分开，插入一发子弹），或者是看起来像巨大左轮手枪的鼓式发射器。这些左轮手枪通常是通过泵的动作来推进，而不是像传统左轮手枪那样通过扳机来推进。根据不同的型号，这些手枪往往能装4到6发子弹。有些手枪有膛线，可以旋转弹丸以提高精度。在国际上，许多这类枪都有木质枪托，看起来更像传统的步枪，而在美国看到的大多数是“战术”风格的枪，除了枪托之外还有手枪握把以及垂直的前握把——

如果没有特别的许可，平民持有是不合法的。

发射器也可以安装在步枪的枪管下，而不是作为独立的装置。这种方式在军事情况下很常见，但在警察部门似乎并不常见。

[image] 多管发射器

霰弹和榴弹

在本条中，我们将设计为从发射器发射的“霰弹”与设计为用手投掷的“手榴弹”区分开。实际上，并没有这样明确的区别。有些武器被设计成用手投掷或滚动，而另一些武器则被设计成装入多管发射器—— 但有些武器是为这两种形式设计的。

手榴弹通常用于散播化学剂和/或冲击弹药，特别是橡胶球。其他手榴弹是“分散注意力的装置”，一般称为闪光弹。许多手榴弹结合了这些功能。

我们发现至少有三种警用手榴弹的主体样式。有球式手榴弹，它看起来像一个经典的棒球式军用手榴弹，被设计成可以投掷或滚动。这些通常包含橡胶球冲击弹药，可能搭配化学武器，而其他的则是传统的烟火催泪弹。有“低滚”榴弹，这是一种圆柱体，末端呈大六角形，可将手榴弹的滚动距离降到最低。还有普通的罐装手榴弹，这似乎是最常见的样式。这些可以是任何直径的，但37/38毫米、40毫米、45毫米和60毫米似乎是最常见的。

毒气弹和毒气罐可以通过多种方法散播化学制剂。最常见的是经典的烟火散布，它的工作原理是在罐内生火，以烟雾形式释放化学剂。这些罐子非常热，可能会产生火花并引发其他火灾。

另一种分散方法是气雾剂分散（有时称为“无焰驱逐”），这种方法在OC罐中的使用频率高于CS罐。这种方法释放的东西更类似于雾气而非烟，更常用于室内，而在室内使用烟火罐则不太方便。就我们所能确定的情况而言，这些装置一般不常在室外使用，因为它们产生的化学剂浓度较低。

[image] 一个瞬间爆炸的榴弹

最后，还有瞬时爆炸罐，这种爆炸罐一次爆炸，以粉末形式释放其有效载荷。这种爆炸罐是为室内或室外使用而设计的，但由于尘埃容易被风吹散，它们主要用于对付密集的人群，而烟火榴弹由于有可能产生反弹或有可能引起意外火灾，因此效果较差。这些气罐由于沿边开裂，事后很容易识别。

毒气分散罐通常被设计成可分离成若干个子弹药，如国防科技公司的“三联追击器”可分裂成三个较小的催泪瓦斯罐。这样做的目的是为了让抗议者更难以快速把它们扔回去或用水浇灭。

[image] “三联追击器” [image]

低杀伤力榴弹一般像任何军用榴弹一样装有引信。虽然引信可以有不同的长度，但我们发现两秒钟的延迟是很常见的：在引信点燃前延迟1.5秒，然后0.5秒的引信本身。至少在某些型号上，引信组件在有效载荷被点燃之前就会自行弹出。

有些榴弹配有额外的安全夹，防止在携带手榴弹时意外拉断引信。有的带有防水弹体，适用于高湿度环境。有些，特别是闪光弹，是可以重新装填的。人们报告说，看到警察在抗议活动结束后对该地区进行梳理，并捡起某些废旧的弹药。他们这样做有可能是为了掩盖一些特别恶劣的武器（如**DM毒气**）的使用，但也有可能是在回收可重新装填的榴弹。

榴弹也可以用“指令启动”而不是用引信点燃。这种系统似乎在战术情况下更常见，比如房屋突袭，而不是在更有活力的抗议活动中。这种系统是在榴弹上加装一个管子，以便能够瞬间远程引爆。

[image] 2020年夏天，一名联邦官员使用烟雾榴弹袭击了波特兰的美国公民自由联盟的法律观察员。

喷雾器和雾化器

除了发射榴弹罐以烟雾形式释放化学品外，警察还用手持设备直接用化学品喷洒人们。我们在研究中发现的两种化学品是OC（胡椒喷雾）

和CS（一种催泪瓦斯），但几乎所有的化学制剂都可以被喷雾和喷洒。

根据制造商、化学刺激物和喷雾模式，这些可以采用任何数量的推进器，有许多喷雾模式，从简单的“流”模式到雾（或“蒸汽”），甚至泡沫。

化学喷雾与分散粉末状刺激物的烟火法不同，一般是将化学品的液态形式喷雾化。这可能是水基或油基的；因此，化学武器防护应针对油基微粒进行评级（P100过滤而不是N100过滤）。雾化器也使用液态制剂，但以烟火方式 (如雾化机的方式)而不是使用气溶胶气体将这种液体气化。

化学喷雾剂有一系列不同的浓度，在没有研究的情况下，很难预料到执法部门正在使用的是哪一种。更为复杂的是，众所周知，OC（最常见的喷雾刺激剂）的强度很难确定。制造商的声明不受监管，而且在特定的OC气体变体中可能存在许多不同类型的辣椒素。每个制造商的武器系列中可能存在内部一致性，但仅此而已。一个制造商的2%的喷雾可能比另一个4%的喷雾更强大。这些数字本身几乎毫无意义。

小的手持式罐子，顶部有一个按钮，似乎10–12英尺的准确度，而较大的罐子与触发器组件似乎是精确到15–20英尺，虽然这在不同制造商之间有所不同。许多喷雾系统还包含可见的或紫外线反应染料来标记目标。紫外线染料在民用自卫喷雾中特别常见，而西雅图和其他城市的警察已知使用可见的染料来标记示威者以进行逮捕。

有一些较大的罐子，其工作原理与小罐子相同。这些通常看起来更像全尺寸的灭火器。还有一些背负式装置，有单独的喷头和罐子——有抗议者称之为“捉鬼敢死队”。这些装置可以使用粉末或液体化学品；至少有一种型号的有效范围是45英尺。有人看到波特兰警方将化学品雾化器藏在一个没有标记的黑色背包里，背包底部有一个连接到软管的喷头。

[image]

还有一些装置，看起来像雾化器和鼓风机的混合体，是以空气为动力的，目的是使大面积地区充满毒气。和背包式喷雾器一样，这些装置

一般是设计用于监狱，而不是示威游行。然而，正如我们最近所看到的，防暴警察往往会使用任何他们可以使用的武器镇压抗议者。

[image]

最后，化学武器有时会与水混合，通过消防水龙或水炮撒出去。在2020年波特兰的抗议活动中在美国使用。附近一棵树上的化学灼伤符合氯气中毒状况，这可能是化学药剂过期的结果。香港、泰国和土耳其的抗议活动中都曾使用过这种化学武器散布的手段；据推测，任何使用水炮对付示威者的国家都有可能使用这种手段。

[image] 2020年夏天，联邦部队用雾化器毒害了波特兰市中心

蜡烛

一百年前，化学战刚兴起的时候，一些有毒气体是通过“蜡烛”来分散的，蜡烛燃烧后会释放气体。从功能上看，这和现代催泪弹是一回事，它是利用烟火来散布化学粉末的。“催泪蜡烛”这个词可以用来形容任何烟火催泪弹罐。

然而在2020年的夏天，我们看到不是警察就是联邦特工，在波特兰的街道上走来走去，在棍子的末端拿着一个燃烧的物体，烟雾从上面涌出。

[image] 2020年夏季，警察在波特兰喷洒催泪瓦斯

我们不知道这是否是化学制剂（可能）或惰性烟雾，但感觉值得注意的是，我们遇到的唯一一种催泪瓦斯，就是为这种散布形式设计的，就是DM瓦斯，抗议者认为波特兰使用的呕吐瓦斯。这将标志着对抗议者使用的化学战形式的重大升级。

【注：亚当氏毒气或二苯胺氯胂，简称DM，是一种有机化合物，可作防暴用途。DM属于化学战剂，被认为是呕吐战剂或者喷嚏性毒气。】

[image] 民用胡椒喷雾

化学武器

与所有其他许多低致命性武器一样，化学品类别之间的区别实际上相当模糊。

传统的说法将化学品防暴武器分为两类：催泪瓦斯和胡椒喷雾。虽然这些区别存在，但并不明确。如果我们把“催泪瓦斯”想象成烟雾或灰尘，把“胡椒喷雾”想象成化学喷雾，这其实是一个扩散方法的问题，而不是实际使用的化学品。

我们将在此讨论七种不同的化学品。虽然已经实际开发了大约15种化学品，但我们将重点讨论最常见的化学品，这些化学品要么是已知的，要么是被用来对付示威者的，至少是被广泛怀疑被用来对付示威者的。

在这七种中，有五种通常以气体形式散布，有两种通常以化学喷雾形式出现。但是，几乎任何化学品都有可能通过任何方式被散布，我们已经看到了不少交叉使用的情况。

五种催泪气体，简单来说就是：

- CS气体，是最常见的催泪气体；
- CN气体，是一种过时的催泪气体，毒性较大，效果较差，但目前仍在生产和商业上销售；
- CR气体，以难以置信的无法清洗而闻名—— 这种气体会使你的皮肤比遭遇其他气体烧得更厉害，并被怀疑在使用，但没有被列为商业用途；
- DM气体，近乎神话的“呕吐瓦斯”，警方被怀疑使用，虽然还没有确凿的证据；

- 还有MPK气体，据我们所知，它只在俄罗斯使用，但一些读者可能会感兴趣。

此外两种胡椒喷雾剂是：

- OC，就是常见的“辣椒喷雾”，是用辣椒制成的；

- PAVA，一种合成形式的OC，似乎以非常相似的方式发挥作用。

在本文中我们将在很大程度上把这两者混为一谈，因为我们很难确定它们之间的任何重大区别。

最早的自卫喷雾剂实际上是用CN气体填充的，但**OC**通常在使目标失能方面更有效。有填充CS、CN和OC的喷雾器；也有填充OC和PAVA的催泪弹。

就控制人群的表面目的而言，**OC**（或**PAVA**）是最有效的催泪瓦斯剂。它起效最快、破坏力最强、毒性最小，而且受害者恢复得更快。CS气体排在第二位；它的使用更为传统，也最为广泛。

无论从哪个角度看，除了OC或CS之外，其他催泪剂都没有什么用处，即使从国家主义的角度看，也只是用来惩罚和毒害人。它们都是过时的和残酷的技术。我们这样说并不是为了博取同情或迎合国家的道德判断，而只是想指出，残忍是问题的关键。

[image] 普通胡椒喷雾

战术上的考虑

化学武器被用于若干战术目的。正如我们在使用冲击弹药时发现的那样，警察在许多方面使用这些武器，而这些武器在设计上是不应该那样使用的。一般来说，催泪瓦斯是为了控制人群的行动，或者驱散人

群。催泪瓦斯云是为了阻止人们占领特定区域。警察使用催泪瓦斯引导人群的方式与防暴警察使用的方式大体相同：大多数人会避开催泪瓦斯，并向空气清新的方向移动。在较小的范围内，使用胡椒球和有针对性地远程部署化学武器也可以达到同样的人群控制效果。

喷雾剂往往在近距离使用。在示威活动之外，它们被用来制服个人。在示威活动中，往往不加区分地使用这些武器，以驱散、恐吓或使人群丧失能力。

催泪瓦斯和其他化学武器不是专门为惩罚而设计的：它们不是用来对付被困的人群或被限制的个人的。当然，警察经常这样使用它们。

[image]

为了防止警察达到控制人群的目的，我们干脆拒绝被控制。

这可能需要一定的事先准备。

为了减轻化学武器的影响，个人防护装备是必须的。本系列此前的防毒面具和护目镜指南对此有详细的介绍。

简而言之就是：

- 穿长袖衣服和长裤，尽量减少皮肤暴露在外面的面积；
- 避免戴隐形眼镜；
- 避免使用化妆品和保湿剂以及其他护肤霜，尤其是脂肪类护肤霜；
- 戴上防毒面具，或半面罩呼吸器与护目镜，或戴上湿头巾和护目镜，并保持活动状态。

- 雨伞可以阻挡化学喷雾。在特朗普就任总统的当天，一把伞保护了数十名抗议者，让他们从警察的釜底抽薪、八项重罪和可能长达数年的法庭案件中逃脱。

https://vimeo.com/522867490?fl=pl&fe=sh

在轻度或中度的化学武器攻击中，通常几个人就可以解除或扔回榴弹罐子，而医护人员和其他人则对受喷洒物影响的人进行治疗。只要不影响示威者的目标，就可以继续行动。

不幸的是，化学武器的大量使用将倾向于稀释那些准备不足的抗议活动。

[image]

用湿头巾 (存放在单独的密封袋中) 、或其他个人防护装备可供分发，可以使人群在周围停留更长时间。

扔回催泪瓦斯罐

> “把催泪弹扔回去是不礼貌的 ... 但有时那是爱，有时真正的爱是他妈粗鲁的”—— 安德里亚·吉布森，《礼仪束缚》

抗议者经常将催泪瓦斯罐扔回镇压者的一方。由于催泪瓦斯是以烟火方式施放的，因此大多数催泪瓦斯罐的温度很高，足以引起火灾或烧伤皮肤。

[image]

任何希望处理催泪瓦斯罐的人都应该戴上由防火材料制成的绝缘工作手套。廉价的五金店里卖的那种手套是不够的；气罐曾烧穿了抗议者的手套。合成材料，如果不是专门设计的防火材料，可能会融进人的皮肤。皮革工作手套往往是最简单也是最好的选择。

人们还采用曲棍球棒来回击催泪瓦斯罐而不直接接触它们。

警察可能会在不戴防毒面具的情况下使用胡椒喷雾，但如果他们要对整个地区放毒，他们几乎都会戴上面具，或者轮流换上一排新的穿着防护装备的警察。

[image]

这一点很重要：这意味着，如果您的角色是负责留意警察，您应该能够提前知道他们何时准备对你们施放毒气。当然，我们不是律师，关于允许向警察投掷哪些燃烧物的法律可能因地而异。

只有在意识到周围的环境，并且身后有空地的情况下，才可以投掷燃烧弹。

在扔罐子之前，要注意风向和人们可能很快需要跑去的地方，以及他们目前所处的位置。

[image]

中和催泪瓦斯罐

近年来，世界各地的抗议者一直在学习如何使毒气罐失效，而不是简单地把它们扔回去。这些方法的优点是对抗性较小。

由于大多数毒气罐都是用烟火部署的，所以只需将毒气罐内的火熄灭即可。有一种根本不需要接触罐子的基本方法，就是在罐子上放一个交通锥，然后从交通锥顶部的孔里往里倒水，直到把罐子浇灭。

[image]

一种更精细的方法是用戴着手套的手捡起罐子，然后将其放入一个大水瓶或水桶中。在智利和世界上其他一些地方，反叛社区已经练就了他们的做法，携带大水罐已经成为街头抗议活动中的一个独特角色。

扮演这个角色的人带着一个口子宽大的水壶，里面装着少许小苏打、洗洁精和/或植物油—— 每一种都是1升水加3汤匙的比例。

当一个罐子被发射过来时，他们把它扔进水壶里，然后摇晃水壶，同时用一只手盖住顶部，以防止气体流出。如果您尝试这样做，不要密封瓶子—— 您不会希望它爆炸的。

如果没有其他办法，如果您不准备中和瓦斯罐子，只需用烹饪锅或橙色的交通桶等东西盖住它就可以了。依旧有些气体会泄漏出来，但这会降低它伤人的能力。

化学武器的作用

从理论上讲，防暴毒剂的设计是尽可能让人感到不舒服和虚弱，而不会造成永久性损害。

- 它们会刺激肺部、眼睛和皮肤。
- 它们是催泪剂，会让您的眼睛流泪。
- 您可能会流鼻涕。
- 您可能会有呼吸困难。
- 您可能无法睁开眼睛。
- 有些化学武器几乎立即生效；有些则在接触后几分钟就会影响到您。

有些化学武器在您转移到新鲜空气中很久之后仍会继续刺激您；有些则消散得更快。有些比其他的毒性更强；有些会造成永久性伤害。

我们将分别讨论每种化学物质的具体影响。但简而言之：有时接触防

暴毒剂会让人痛苦和虚弱，特别是当您在没有防护措施的情况下直接接触它们时。在其他情况下，它们可能只是刺激性的。

呼吸急促是接触化学武器导致的一个具体而常见的问题。当这与被毒气的冲击、情况的整体压力和刺激肺部相结合时，有些人可能会觉得自己要晕过去了。

[image]

如果您遇到这种情况，请尝试快速离开施放毒气的区域，以良好的姿势坐起来或站起来，尝试深呼吸。

即使您的呼吸仍然受到限制，额外的氧气也会降低您的环境压力水平，使您能够解决焦虑的一些影响，并降低心率。

如果您看到其他看起来快要晕倒的人，尽量把他们带到有毒区域以外的安全地方，鼓励他们尽可能地深呼吸。

化学武器的另一个目的是恐吓我们。它们被用来阻止我们上街，阻止我们完成目标。如果您还在街头积累经验，建议您和那些在公共秩序方面有相当经验的头脑冷静的人讨论一下，如何应对化学武器袭击的压力。

[image]

如果您是第一次经历大规模的警察暴力事件，而您又可以选择，那么，最好的办法是遵循自己的身体节奏，在压力过大的情况下离开，以便慢慢地、稳定地建立一种平心静气地应对的技能。

如果您的目标是长久地参与社会运动，那么一开始就谨慎一些，总比对自己要求太高，然后有了不好的经历就退出斗争要更好。

这些年来，一些抗议者受到了天下所有镇压手段的打击，并且活了下来。我们有这样的经历，也有和那些在激烈的警察暴力下仍然坚持斗争的人们在一起的经历，都对解除警察武器的神秘感起到了很大的作用。

给那些特别容易受到伤害的人

哮喘病人和其他呼吸困难的人应特别小心接触化学武器。这可能意味着要带上防毒面具，或者一旦看到警察准备使用毒气，就立即离开该地区。在这些化学制剂造成的死亡中，似乎哮喘患者占了大多数。

根据催泪瓦斯研究者 Sven-Eric Jordt 博士的说法，儿童特别容易受到催泪瓦斯的伤害，因为他们的肺部较小，但这并没有阻止联邦官员在美国边境对移民儿童使用催泪瓦斯。

免疫力

关于对CS或OC有免疫力的传言很多，特别是在军界。

有些人似乎对CS气体有天然的免疫力，或至少对它有较强的耐受力。尽管有疼痛和其他影响，确实有可能建立起继续工作的心理能力。但并没有证据表明可以对**CS**或**OC**产生生理免疫力。事实上，恰恰相反，重复接触**CS**毒气会导致过敏 —— 与耐受性相反。

美军士兵在基础训练中会接触到CS毒气，作为 “信心训练” 的一部分，目的是展示他们的防毒面具的有效性。在这些训练中，似乎有一小部分人（根据我们看到的推测，可能有2–5%）对CS的影响有天然的抵抗力。在一个论坛上，我们看到一个对CS毒气耐受性很强的士兵让人用辣椒喷雾喷他，误以为辣椒喷雾（OC）是一回事。事实证明，他对胡椒喷雾没有免疫力。

在任何情况下，经常性地让自己暴露在CS气体中，希望建立起对CS气体的心理耐受性，都是不明智的。暴露在CS气体中会引起一些长期的健康问题。也并没有任何证据表明吃辣椒之类的东西可以增加您对它的耐受性。

一些警察学校显然在教授关于胡椒喷雾的种族主义神话，在没有证据的情况下暗示拉美人和东亚人对胡椒喷雾的耐受性更强 —— 因此，暗示他们需要被喷得更久。这只是几个世纪以来白人至上主义伪科学为残酷行为做辩护的最新成果。

如何治疗化学制剂的影响

根据药剂的不同，大部分化学药剂的影响会在呼吸新鲜空气30分钟后消失。避免揉眼睛！不要戴隐形眼镜！

[image]

用水冲洗眼睛 —— 或者，最好让别人帮您冲洗眼睛。

您给别人冲洗眼睛的最好方法是拿一个运动式的喷水瓶，向受害者睁开的眼睛喷水。

带一个这样的瓶子，只用来冲洗，不要用它喝水，以免唾液污染。

您可以用拇指和食指打开别人的眼睛；如果您有干净的手套，请戴上。

只要让受害者的眼睛睁开一点就够了。

从眼睛内侧，靠近鼻子的地方开始冲洗，然后再向外侧冲洗。

每次只做一只眼睛。要求他们眨眼；提醒他们不要碰自己的脸。根据需要重复多次。

用一定的力气喷洒水：目标是冲掉眼睛上的化学物质。冲洗眼睛不会立即减轻灼热感，但可以使您开始恢复。

要想把泪液和其他污染物从皮肤上弄掉，用肥皂和水清洗。如果气体在您身上干成粉末状（尤其是过期的催泪瓦斯，这种情况更有可能发生），在冲洗前将粉末从皮肤和衣服上刷掉。虽然有人认为水能 “激活” 粉末状的化学刺激物，但经验表明，用水或肥皂和水清除是有效的。

当您在被毒气袭击后遇到别人时，如果您还穿着同样的衣服，或者头发上有残留的毒气，请警告对方离您远一点。您可能不会受到微量气体的影响，但仍可能引发其他人的重大反应，特别是如果他们有哮喘或类似情况的话。如果您和其他人一起进入封闭的空间，这也是一个问题。

当您在接触化学品并离开冲突区域后，脱掉外衣，将其双层打包，直到有机会清洗。淋浴，用肥皂大力擦洗皮肤。当您洗掉头发上的化学物质时要小心：如果有化学物质进入您的眼睛、生殖器或开放性的伤口，会非常疼。

要处理您的衣服，彻底清洗它们，可能要经过多次循环。之后在没有任何东西的情况下运行洗衣机，以清洗洗衣机本身的内部。最好把衣服晾在外面的晾衣绳上，这样任何残留的影响都可以消散。

催泪瓦斯和COVID-19

催泪瓦斯让人眼泪鼻涕一起流，而体液是COVID-19感染的有效载体。出于对最大限度地减少致命疾病传播的考虑，一些本来要对接触化学武器的人进行救助的医务人员开始提倡人们在有能力的情况下，对接触化学武器的人进行自我治疗。如果做不到这一点，在给接触化学武器的人进行治疗时，应该戴上手套、护目镜和自己的口罩。注意尽快清洁和去污。

去污湿巾

执法部门使用 Sudecon 湿巾来清除胡椒喷雾和催泪瓦斯的污染。医务

人员报告说，他们还没有看到并列比较，但相信 Sudecon 湿巾的效果可能至少与皮肤上的肥皂和水一样好。

俄勒冈州波特兰的 Rosehip Medic Collective 公布了一个**DIY**去污湿巾的配方，在2020年夏天，这些湿巾在那里被化学浸泡的街道上被广泛使用。

首先要用：

- 1加仑温水
- 9杯白糖
- 2汤匙柠檬酸

将其充分混合，然后与21盎司的婴儿洗发水混合，轻轻搅拌。将高质量的纸巾浸泡在混合物中，并将它们装入密封袋中，每次几条。这些应该可以保存几天，或者在冰箱里保存几个月。

波特兰的医护人员在制造这些湿巾时，借助了一台小型的滚动机器，使水分分布更均匀；他们希望这能使湿巾保存的时间更长。这也有助于医护人员更快地制造它们。

其他补救措施

人们对化学武器使用了许多不同的补救措施和治疗方法—— 从牛奶到抗酸剂和草药混合物，应有尽有。根据我们与街头医务人员和医生的对话，建议只用水冲洗眼睛，用肥皂和水清洗皮肤。

提倡用水，因为它很容易获得，而且不太可能引起过敏反应。因为它不恶心 —— 被浸泡在牛奶中被捕可不是什么愉快的经历—— 还因为水不会像抗酸剂那样留下明显的白色残留物，而抗酸剂在深色皮肤上

会更明显，并被用来标记逮捕嫌疑人。

如果您强烈认为需要某种特殊的补救措施来治疗接触化学武器的伤害，这就增加了它们的神秘感和它们可能激发的恐惧。但这些刺激性物质并不那么神秘。把它们洗掉，然后去呼吸新鲜空气。即使您不同意我们的观点，不认为水是最好的，也请不要打断有经验的街头医务人员用水冲洗眼睛。

有一种过时的抗议技术（被称为MOFIBA），它使用矿物油来清洁皮肤上的污染物，但它基本上已经被淘汰了，因为，如果施用错误（无论是由于缺乏经验还是动荡环境中精神过于紧张），它可能弊大于利。这里就不详细介绍了。肥皂和水是清洁皮肤是有效方法。如果您有去污巾的话，去污巾是很好的 —— 可能更好，但不是必须的。

额外的护理有时是有用的，无论是在医学上还是在情感上。正如一位街头医生所说，他们把乳液擦在戴手铐的瘀伤上，因为当有人向您展示警察手铐造成的瘀伤时，他们是在向您展示了他们被攻击和绑架的物证。当您检查这些瘀伤并涂抹乳液时，您就会表明发生在他们身上的事很重要，其后果值得小心对待。乳液很可能有助于缓解瘀伤，但表现出关心的行为在此更加重要。

智利的一些抗议者已经采取了将常温茶（由月桂叶煮沸制成的）喷洒到那些遭受胡椒喷雾的人的眼睛里，似乎很有效。这不是机械地冲洗眼睛，而是用小喷雾瓶，作为事后处理，以减轻灼伤，使人平静。

香港一些示威者携带的喷雾瓶中，每**8.5**盎司的水含有**3**茶匙小苏打。虽然这种做法的功效还没有被直接研究，但它与2003年的一项研究结果一致，即CS分子是不稳定的，而小苏打等碱性液体可能会加速这种分子分解的过程。

[image]

日内瓦议定书

也许您听说过，在战争中使用催泪瓦斯是战争罪，是《日内瓦议定

书》所禁止的。这是事实。这不仅仅是催泪瓦斯被意外地卷进了一个不使用化学武器的广泛协议中。它的名字明确地出现在那里。

1925年，在第一次世界大战的化学恐怖之后，38个国家签署了禁止使用化学武器的日内瓦议定书。大多数签署国都认为这包括催泪瓦斯和化学除草剂，不分青红皂白地大量投放。美国政府决定不同意这种解释。在整个20世纪60年代，美国在越南广泛使用催泪瓦斯和除草剂（橙剂）。

如今，《日内瓦议定书》明确规定，催泪瓦斯是被禁止的。

国家元首不希望任何人向他们的平民投掷化学品 —— 但如果这是维持内部 “稳定” 所需的，他们都会支持。所以，是的，国际法明确禁止在战争中使用催泪瓦斯，将其描述为战争罪。但各国政府都同意，对我们这些公民使用催泪瓦斯是可以的。

化学制剂的种类

我们在这里回顾一下比较常见的化学制剂的特性和作用。

1、CS毒气

CS气体（邻-氯代苯亚甲基丙二腈，C10H5ClN2）是最常见的催泪剂。两位美国科学家 Corson 和 Stoughton 是第一个合成它的人，他们以自己的名字命名。直到20世纪50年代，它才被武器化为催泪瓦斯。

CS气体主要存在于催泪瓦斯罐中，但它也出现在喷雾剂中，或掺杂在整个冲击性武器阵列中。

CS毒气被认为比CN毒气的毒性要小得多，后者在使人致残方面更有

效。它的毒性可能比OC更大，但致残性更小。

我们知道**CS**会引起心脏和肝脏问题。我们知道强烈接触会造成化学灼伤和疤痕。但还有其他更多的问题。

就直接致命性而言，据推测，在封闭的空间内，CS可能会致死；抗议者将起义期间解放广场上的几起死亡事件归咎于CS。但这一点尚未得到证实。与其他化学制剂相比，CS毒气似乎没有那么大的杀伤力。然而，它的长期影响却令人担忧。

大多数关于CS的毒性报告都是50多年前的，新的研究有些罕见。美国军方通过研究士兵暴露于CS毒气室前后肺部问题的发生率，越来越多地发现CS毒气与持续性肺部问题之间的联系。

CS气体具有致癌性 **——** 也就是说，它可以改变你的染色体。这主要影响到生理期的人。科学界对这些影响的研究一直很缓慢，但大量的故事描述了流产、出血过多、痉挛、血栓以及接触CS气体后的癫痫发作。

CS气体（不同于OC和俄罗斯的催泪瓦斯MPK）一般认为对狗、熊和其他一些哺乳动物的效果不明显。但也有研究表明它能够杀死狗。来自土耳其的轶事报告描述了CS气体杀死了成千上万的鸟类和导致流浪猫失去视觉。

和所有的化学武器一样，警方使用的**CS**并不是“纯”的，而且它掺杂的其他化学品也可能是有毒的。我们认为，液体/喷雾的版本，至少是英国警方经常使用的版本，其中采取了甲基异丁基酮（**MIBK**）作为溶剂。**MIBK**本身是有毒的，可以引起肝脏和肾脏问题。

至少在得克萨斯韦科市的围剿行动中，美国政府在使用CS的同时，还使用了有甜味的溶剂二氯甲烷进行雾化。这东西具有致癌性。

一些抗议者报告说，2009年在匹兹堡举行的20国集团峰会抗议活动中，至少有一些气体闻起来像香蕉糖，很可能是二氯甲烷。

[image] CS毒气罐

2、CN毒气

2-氯苯乙酮是有机化学中常用的一种化学品。当它被用作催泪瓦斯时，它被称为CN气体。它最早是在第一次和第二次世界大战期间作为催泪瓦斯开发的，尽管不知道它是否被使用。

CN 气体可通过任何一些警察武器制造商在市场上买到。它比CS或OC更不常见，但可以在催泪瓦斯罐、喷雾器和整个冲击性武器中找到。

在OC被开发出来之前，CN气体是第一个品牌的自卫喷雾剂 “Mace” 的有效成分。

CN 气体已导致至少5人因心脏损伤或窒息而死亡。它还造成了接触性皮炎——有时是永久性的！——数量不详的警用化学武器意外泄漏到他们身上。如果它能以这种方式伤害警察，它也能伤害我们。

3、CR毒气

CR气体($C_{13}H_9NO$)是一种催泪瓦斯制剂，它于20世纪60年代在英国研发，因其不仅能伤肺、伤眼，还能让您全身如同被扔进一片荨麻中，而获得 “火气” 的绰号。据说它的味道很甜。

[image]

据称，**CR**气体的药效是**CS**的**6–10倍**，虽然我们找到的所有文件都说它比CS “毒性小” ，但众所周知，它能够通过窒息或肺水肿（液体充满肺部）致人死亡。

CR气体最糟糕的一点是，它比其他防暴毒剂更难消除污染。它可以在表面持续存在长达**60**天。

我们没有发现任何制造商宣传任何含有CR气体的产品。

波特兰的一些抗议者猜测，他们可能接触到了CR气体，因为他们接触到的一些气体对他们的汗水反应特别强烈。该理论认为，联邦特工厌倦了戴着防毒面具的抗议者，利用了一种即使对戴着面具的人也同样会造成严重痛苦的化学武器。这些联邦特工可能有机会获得CR气体的旧仓库，也可能不需要像地方警察一般通过面向公众的商业渠道购买。

然而，CS气体（或许尤其是过期的CS气体，可能会造成较大的片状物，在皮肤上持续的时间更长）也会与汗液发生反应导致灼烧。化学家和其他人员目前正试图弄清CR或DM是否一直在波特兰被使用。

[image] 一种神秘的绿色气体被警察用来袭击波特兰的抗议者，部分成分被确认为HC毒气。

4、DM毒气

DM毒气 (亚当氏毒气、或二苯胺氯胂) 是另一种基本过时的、特别恶毒的催泪剂。德国和美国的化学家在上世纪**10**年代就独立研制了它。它最初是用 “蜡烛” 燃烧来分散气体的。

DM毒气作为防暴剂特别无效，因为它的效果需要5–10分钟才能显现。 它开始时和其他催泪瓦斯一样，对眼睛和肺部有刺激性，但会发展成恶心、头痛和持续呕吐。

DM毒气在美国最臭名昭著的使用是1932年，4.5万名第一次世界大战的老兵及其盟友在华盛顿举行示威。有目击者说，毒气使两名幼童窒息，不过历史学家一直无法证实这一点。

有人猜测2020年夏天联邦特工在波特兰使用DM毒气，但仍无法证实。有传言描述可能是DM毒气的绿烟，还有报道说一些催泪瓦斯让人呕吐。到目前为止，没有人能够证明也没人能反驳这一点，尽管一部分在波特兰利用的绿色气体已被确认为HC毒气。

[image] 有毒的DM气体被用来瞄准那些参加抗议的一战退伍军人。

5、胡椒喷雾：OC

OC（辣椒油素）是我们所知的唯一一种有机提取的防暴剂。它是从辣椒的活性成分辣椒素中提取的。

就防暴剂的表面目的而言，OC似乎是最有效的：它的刺激性和致残性大大高于**CS**或**CN**气体，起效时间也比这两种气体快，而对接触它的人造成的长期不良健康影响显然要小得多。

OC最初是作为胡椒喷雾剂推出的，但越来越多地出现在催泪瓦斯的变体中，出现在催泪瓦斯榴弹中（包括慢速燃烧和瞬间尘埃云），并掺杂在整个冲击性武器的投放中。

[image]

为了避免我们把OC描绘得太过美好，必须说明：它也可以致人于死地**——** 特别是那些接触到大量**OC**的人，比如当警察用**OC**折磨被限制的被捕者时，这是一个很常见的程序。特别是，它可以通过 “严重的急性支气管痉挛” 使哮喘病人的肺部与空气隔绝而死亡。

喷雾状的OC通常悬浮在乙二醇中，而乙二醇本身是比较无害的。

6、PAVA

PAVA (N-香草基壬酰胺、天竺葵酸香兰基酰胺) 是一种(通常)合成形式的OC，在英国比在美国更常见，在英国它是最常见的胡椒喷雾剂。

PAVA 确实是天然出现的，但厂家一般都是合成的。它比OC更热稳定。还没有发现PAVA和OC的毒性有什么特别的区别。

大多数PAVA喷雾剂都悬浮在水乙醇中。在其他情况下，它是悬浮在单丙二醇、乙醇和水的混合物中，称为 PAVA 2。 PAVA 1 是易燃的，而 PAVA 2 不是。两者都不是由我们已知的特别有毒的化学物质

制成。

7、MPK

西方读者不太可能接触到 MPK (N-nonanoylmorpholine)，这是俄罗斯使用的一种催泪瓦斯，很容易使人丧失行动能力。它的毒性不如其他化学药品，所以一般是与CS或CN气体混合使用。据报道，它的毒性大概比与之混合的化学品要低。

8、烟雾弹

警方使用的许多霰弹只是烟雾弹。警察用烟雾弹来标记、区域，隐藏自己的位置和行动，在人群中造成恐慌，并可能使指向他们的激光发生折射 (我们不确定这是否有效，因为关于激光的信息有很多不一致)。大多数化学武器制造商还提供各种罐装和手榴弹的烟雾弹版本。

许多军用型烟雾弹，称为**HC**或**HCE**榴弹，含有六氯乙烷。六氯乙烷通过皮肤吸收有毒，抑制中枢神经系统；据推测是一种致癌物。20世纪20年代中期，俄勒冈州波特兰市的联邦特工使用了含有HC的榴弹。根据一位研究人员的说法，HC不再在美国生产，而是作为其他化学过程的副产品收获。虽然它有毒，但似乎比警方采用的其他化学武器安全得多。

“Saf-smoke” 榴弹，即国防科技公司生产的款式，被宣传为危险性较低。“Saf-smoke” 和其他竞争品牌的烟雾弹的实际内容是专有的，不能立即提供审查。

[image] Saf-smoke榴弹

9、闪光弹

这些装置被制造商称为 “分散注意力装置” 或 “迷惑装置” ，更常见的

是闪光弹或眩晕榴弹。它们会产生强烈的闪光和巨大的爆炸声以及一定的震荡力。

[image]

光线（高达800多万坎德拉—— 相当于800万支蜡烛的亮度）使观看者失明约5秒钟，并造成严重的后遗症。其音量约为160–180分贝，比你可能听到的任何枪声都要大；这会使附近的人失聪，扰乱内耳的液体，有时还会引起头晕。

警察偶尔会在希望打得示威者措手不及的时候，将其与警棍或其他冲击性武器一起使用。但归根结底，就像许多警察的战术一样，这些都是恐吓人们服从的方法，而不是直接强迫人们服从的方法。

闪爆榴弹一般由实心钢或铝制成，设计上不会因引爆而破碎。它们中的许多都是可以重新装填的。

有些闪光弹是 “空中警告/信号” 弹药，设计为用于向空中发射，在人群上空爆炸。这些榴弹可以有或没有化学有效载荷；每发子弹的射程不同，从50米到300米不等。也有适用于12口径猎枪的版本。

至少有一家制造商表示，在闪光弹引爆的地点周围应该有一个5–6英尺的清晰区域；但警方仍然经常向人群中投掷、发射和滚动这些弹药。虽然有些闪光弹内装的是橡胶球弹药，但大多数闪光弹的设计不会通过撞击造成伤害。然而，它们可以使人致残或死亡，通常是通过燃烧。据了解，它们也会引起火灾，特别是在室内使用时。

[image] 闪光弹

收集废旧弹药

由于对纳税人花钱让警察购买向公民开枪的武器的监督太少，信息也太少，因此，抗议者采取了记录废弹壳的办法，以了解警察发射的是什么东西。收集废旧弹药有助于进行有用的模式分析。一些城市有人愿意为此目的来收集弹药。如果您所在的城市没有人从事这项工作，

可以考虑自己去做。

波特兰的警察似乎确信—— 或者说正试图说服人们—— 捡拾废旧弹药"是一种犯罪"，他们威胁要向任何被发现这样做的人发射更多的弹药。目前还没能弄清楚这到底是什么罪。

警方的弹药经常被发现未爆炸的哑弹。我们不清楚这是因为这些弹药没有正常部署就发射了，还是警方只是不小心把弹药丢在了地上。

[image]

当打开一袋废旧弹药时，有可能会受到毒气残留的二次影响。考虑将它们装入密封袋中双层袋存放。只有在戴着手套和穿戴防护服的情况下，才能在露天环境中处理这些弹药。

标记

警察有时试图给参加示威或涉嫌犯罪的人打上记号，希望以后能逮捕他们。在某些情况下，警察可能只是利用标记来吓唬我们，让我们相信他们会来找我们，希望限制我们选择在街头做什么。

据了解，警方使用标记的次数远远多于这种标记后来被用来识别人们的身份以便逮捕或在法庭上作为证据的次数。我们希望听到任何有更多关于标记的信息的人，无论是通过经验还是研究。

有报告称，至少在2003年迈阿密反对美洲自由贸易区部长级会议的抗议活动和同一时期的反对伊拉克战争的抗议活动中，警察就使用了胡椒弹做标记。

已经能够确定至少有七种警察给人做标记的手段：

- 恶臭剂

- 暂时性粉末
- 可清洗的涂料
- 难以清洗的涂料
- 紫外线染料
- DNA标记

很可能还使用了彩色的、可见的染料。这些染料往往与其他效果搭配使用，如豆袋弹装上荧光绿粉或**FN303**弹，给冲击性武器添加油漆或染料。我们还收到报告说，波特兰的警察从屋顶上照射绿色激光，将抗议者标记为冲击性武器发射的目标或逮捕的目标。

市场上似乎只有一种恶臭弹，即安全设备国际公司生产的40毫米BIP恶臭弹。它的目的是通过气味来标记人们，同时也能起到震慑人群的作用。这种气味被福克斯新闻形容为“鸡蛋沙拉遇上垃圾”，据说散得相当快。

标记粉、油漆或染料可以通过任何施放化学品的手段来使用。漆弹枪、霰弹枪和多管发射器都有标记弹，我们也听说过警察在水炮上添加油漆或染料的报道。

我们还没有找到标记弹中常见的油漆或染料的具体成分信息。一些制造商将他们的产品分为“可清洗”、“难以清洗”和“紫外线”，或者分为“粉末”和“液体”。例如，Security Devices International, Inc. 声称，他们的液体标记弹会留下“半永久性污点”，或“在目标和衣服上保持24小时”。该数据表将其内容称为惰性材料的专有混合物。其他公司则没有提供更多信息。

去除印记

处理衣服上的印记、避免确定您是嫌疑人的最简单的方法就是，把衣服扔掉。您应该根据衣服对您的重要性以及您担心自己会因为什么而被逮捕来做出这个决定。一个法庭案件通常比一件衣服更昂贵。您也可以把一件衣服放在某个地方—— 例如，放在灌木丛或垃圾桶里，然后再回来看看是否能找回它。

被称为可清洗的油漆和粉末应该是最容易清除的。去除衣服上的水性涂料的方法之一是让涂料干透，然后用黄油刀或勺子尽量刮掉；然后用手洗物品；将一半洗涤剂和一半水混合，将其擦入污渍中。然后冲洗，再重复最后一步，直到污渍消失。在最坏的情况下，可以尝试使用少量丙酮（指甲油去除剂）或摩擦酒精 —— 但要注意，这可能会损坏物品。

油性涂料，可能会用到 “难以清洗” 的涂料，可以通过混合橄榄油和洗碗皂，在皮肤上打出泡沫，然后冲洗干净，必要时重复进行。您可以将衣服内侧朝外放在一堆抹布或纸巾上，然后将松节油或另一种油漆稀释剂从污渍后面倒在布料上，用抹布擦拭，就可以去除衣服上的油性油漆。一旦这样不再有油漆溢出来，就把洗洁精搓进污渍里，然后把衣服放在热的肥皂水里过夜。第二天早上彻底冲洗，然后把衣服扔进洗衣机。

紫外线墨水也可以从皮肤和衣服上去除。在某些方面，它可能比其他墨水更容易清洗，因为除了在紫外线下，它不会真正干燥（我们不确定阳光下的紫外线是否会导致它干燥）。大多数UV墨水似乎是酒精溶解的，所以使用摩擦酒精甚至发胶应该有助于从皮肤上去除它。我们看到的其他建议包括用稀释后的漂白水清洗，或者用糖和洗碗液的混合剂擦洗皮肤。还有一些人坚持认为，热肥皂水和大量的磨擦就可以了。您可以尝试用热水反复洗衣服，边洗边用紫外线手电筒检查。

有便宜的小手电筒，有普通紫外线的LED灯。通常，它们被从事门禁工作的员工用来寻找手印，或者被用来检查被褥是否有臭虫。

[image]

返回：🖊痕量证据鉴定

DNA标记

实际上，有两种不同的东西被称为DNA标记。第一种是一种化学武器，通常是一种喷雾剂，其中含有不同金属和其他材料的独特混合物，作为一种化学指纹，可以在以后被识别。这种标记只把DNA这个词作为广告术语。每一个瓦斯罐或每一批瓦斯罐都可能含有自己独特的指纹，尽管我们还不能证实这一点。

另一种风格的DNA标记使用的是DNA的字面意思。这种**DNA**标记系统是用合成的**DNA**标记目标，这种**DNA**可以在衣服或皮肤上存活数周。

这两种DNA标记系统的工作原理是一样的：如果以后通过这些标记的方式确认某人的身份，就可以在法庭上提供具体的证据，将他们与潜在的“犯罪行为”联系起来。

我们有充分的理由相信，警方正在使用这两种方法中的一种或两种对付抗议者，尽管很难知道是哪一种，也很难知道他们何时使用。例如，由 Security Devices International 公司生产的40毫米DNA法医标记轮，使用了一种“水中植物加密标签剂”，我们相信它指的是实际的合成DNA。

我们所能找到的所有DNA标记材料似乎都是悬浮在UV墨水中进行散播的，尽管不知道它们必须这样做的理由是什么。

截至本文撰写时，还没有听说任何与2020年抗议活动有关的涉及DNA标记的逮捕或法庭案件。大多数事后对抗议者的重罪逮捕似乎不是这种标记，而是直播的镜头和社交媒体帖子。

请注意，这并不意味着DNA标记没有被使用，也不意味着它在未来不会被使用。

在推特上，明尼阿波利斯警方曾公开讨论过使用DNA标记喷雾，尽管他们并没有特别声称对抗议者使用过。他们也有可能是把“紫外线标记”和“DNA标记”混为一谈了。

[image]

返回：DNA

去除DNA标记

由于所有现有的证据都表明，DNA标记是在紫外线染料中进行的，因此似乎可以用类似于去除紫外线染料的方法来去除。大多数制造商声称，标记可持续“数天”或“禁得住数次清洗”，但至少有一家制造商声称可持续“数周”。

一家制造商，Security Devices International（SDI），声称它在人身上能持续**3–5**天，但在衣服上能持续**2–5**年。

[image]

来自波特兰的传言称，合成DNA会被紫外线降解。有人建议，任何不想破坏或扔掉的衣服—— 例如，防弹衣 —— 都应该在阳光下放置几个小时，有人建议定期翻动衣服，以确保物品的所有部分都暴露在阳光下。

阳光对盔甲的塑料聚合物不利，尤其是软质防弹衣，所以对于某些材料可能不建议这样做。

人们还建议使用酒精或双氧水来分解**DNA**标记，但这可能也会使材料降解，特别是在双氧水的情况下。

这一切都取决于摧毁您在特定时间在特定人群中的证据有多重要。根据风险的严重程度，您可能会需要更换所有受影响的衣服，并花相当多的时间清洗和摩擦—— 或者您可以简单地清洗所有东西几次，洗几次澡，然后用紫外线灯检查自己。

SelectaDNA

也许第一个开发出供警方使用的合成DNA标记的公司是英国的SelectaDNA。

SelectaDNA 公司直接向消费者出售DNA标记喷雾、凝胶和其他设备，用于家庭安全。他们还出售杀伤力较小的**.68**口径空气动力武器，一种是步枪，一种是手枪，用于向抗议者发射**DNA**标记弹。这两种枪的有效射程为**30–40**米，使用**8**发弹夹和**20**发一次性**CO2**弹。它们是半自动的，可以在一秒钟内发射**6**发子弹。每个都配备了一个摄像头。目前还不清楚 SelectaDNA 颗粒是否可以被其他.68口径气枪发射。

每包16颗子弹都有唯一的编码。理论上，这意味着警方可以做的不仅仅是争辩 “这个人在我们用绿色漆弹射杀所有人的示威活动中，你可以从绿色油漆中看出”—— 他们可以声称 “这是我用这16颗子弹中的一颗射中的人，正如我的步枪相机的时间戳上所记录的那样” 。

[image]

合成的DNA标记可以用紫外线灯在人的身上检测到，或者由经过特殊训练的狗闻到。据推测，这些狗闻到的是紫外线墨水，而不是DNA本身。

[image] SelectaDNA 已经在英国引起争议

[image]
[image]

让监视摄像头失明：示威参与者指南S05E11

[image] 关键词	地形侦查 监视器 进攻
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训 ；[image]反攻 [image]监视器排查 ；周密的行动计划 ；[image]户外无设备对话 ；[image]地形侦查
[image] 创建时间	2025年1月14日
[image] **Description**	行动安全性

最好的防御就是主动进攻。

- Table of Contents

  摄像头 1
  摄像头2和3
  一个人的行动
  摄像头 4、5和6
  地点，地点，地点
  摄像头 7和8
  摄影头9
  新工具
  摄像头 10、11、12和13
  摄像头14、15、16、17、18
  摄像头 19、20、21、22
  侦查

[image]

“老大哥正在看着你”。这曾经是来自荒诞未来的威胁，而如今，这是一个普遍的现实 —— 我们所有人都通过使用智能手机和社交媒体参与其中了。

然而多年来，一股反叛的暗流一直在反击监控，摧毁监控摄像头行动的盛行在社会控制系统中凿出了一个洞。在下面的叙述中，一位匿名研究者发动了一场针对监控基础设施的个人战争，测试了最近从希腊、斯洛文尼亚、到智利和香港的社会反抗运动所采用的一些相同的战术 —— 其中穿插了视频。

本集和前几集的内容有所不同，它并不是具体的战术介绍，虽然包含了一些技巧和思考（黑体字部分）；相反，它旨在展现反抗者打击监视的行动力，希望能由此激发您的创意，开发出适合您本地的、更好的新战术 —— 而您并不需要公开您的创意，只要去实践它在您的行动中，我们所有人都将通过您的成功获得学习。

这篇文章来自美国，以第一人称叙述。

（激光可以让监控摄像头失明吗？是的，可以。）
https://youtu.be/wREpnGqEhSM

自从相机变得足够移动化，可以在未经人们同意的情况下对他们进行拍照，驱赶摄影师就成了人们的一大消遣。从被狗仔队追捕的名人到不满新闻团队侵犯其隐私的平民，再到不想被抓捕的示威者，每个人都讨厌举着相机到处拍摄别人的家伙。

但是，当那个把摄像机推到你脸上的人并不站在那里—— 这里只有摄像机和你的时候呢？即使在我们最无辜的情况下，也很难不觉得自己是个嫌疑人。的确，对于通过摄像头看世界的监视者来说，每个人都是嫌疑人。

这些想法一直在我的脑海中流淌，那天我偶然发现了一个名为“Camover 2013” 的 Youtube 视频。我看到德国人在他们的城市里跑来跑去，拆卸监控摄像头、砸烂监控摄像头，描画监控摄像头的位置。他们说这是一个新游戏，并挑战其他人加入。

（Camover 2013是一场在全国范围内进行的竞赛，参赛队试图摧毁

尽可能多的监视摄像机）
https://youtu.be/9GCsd2TJKjQ

摄像头 1

几周后，我和一个朋友一起外出，寻找可以悬挂横幅的地点。当我们来到一个可以俯瞰市中心主要地带的屋顶边缘时，我们发现自己并不孤单。同样在建筑的边缘上，树立着一个监视摄像头，电线引入墙上的一个洞。我的朋友对这个摄像头发表了意见，但我转移了话题，决定如果要回来找它，还是不要让他人知道比较好。

每个星期天，我的朋友们都会聚在一起看卡通片。那天我实在是顾不上看节目了，我借口要打扫房间就溜了出去，回到自己的屋子。我换上一件好久以前别人留在那里的旧风衣，戴上黑色的手套，一顶棒球帽，还有一些深蓝色的牛仔裤【就是看起来尽可能普通】。我拿起一个帆布购物袋，把那周早些时候从工作用品柜里拿出来的一些剪线钳放进去。我骑着自行车来到离目标几条街的地方，把车停在那里，然后步行靠近，用头巾蒙住脸，帽子拉得很低，以避开附近的其他监控摄像头。

我爬上消防通道，蹬着空调，最后上了屋顶。我蹑手蹑脚地走到那个摄像头的后面，双手抓住它，把它从支架上拧下来，用剪子剪断了电线。我匆匆把相机和剪子塞进包里，然后撤退到我的自行车停放的地方。

在这之前我从没做过这样的事，直到回了家也一直在激动中。我知道下个周末我还会再来一次，我也知道下次会是哪台摄像机。

希腊
https://youtu.be/4JCtXieRNRg

摄像头2和3

我工作的地方就在一家咖啡馆的隔壁，这家咖啡馆在过去几年里生意

一直很好。主人做得不错，唯一阻碍他们的是他们位于 Krusty Burger 旁边，那里有很多黑人青年出没，所以他们在外面装了很多监控摄像头。其中一个摄像头直就指向我在后面抽烟的地方。每天它都会盯着我，我抽烟的时候会尽量不看它。

拆掉这个监视摄像头唯一的麻烦在于，这个摄像头和其他摄像头在一起，基本上都是互相监视的。我必须到屋顶去，但我能看到的唯一能上到屋顶的方法就是在我想要拆掉的那个监视摄像头的正下方。我花了整整一个星期的时间在脑海中演练着各种情景；到了行动的时候我几乎觉得自己已经做过很多次了。

我骑上自行车，把车停在距离目标地点一个街区外，然后步行过去。

在到达现场之前，我躲在栅栏后面，在脸上系了一块头巾。即使戴着帽子和头巾，我还是觉得有点不放心 —— 相机支架的扭动和断裂发生得太快了，回想起来我真的不能确定在剪断电线之前有没有不小心对着自己。如果审查录像带的人最后看到的是我的蠢脸呢？

也许这种情况没有发生，但关键是我犯的任何错误都会被记录下来【记录分析经验教训】。

蒙着面，我迅速走近，把咖啡馆后面的一堆旧椅子搬到墙边，然后爬上去。到了屋顶，我迅速绕到另一台指向同一条巷子的摄像机前，剪断了电线，并把它扳倒，然后在第一台摄像机上重复这个过程。然后我又爬下来，把椅子放回原处。

我骑车走了，把摄像头藏起来，换了衣服。然后我去了街对面的酒吧，等着看是不是会有警察来。我想知道那些摄像头上是否装上了警报器。没有人来。

[image]

一个人的行动

我被这种冒险迷住了。我每周都在为这件事进行策划、心理排练。这个过程发生了两个显著的心理转变。

首先，我与监控摄像头之间的互动发生了变化。以前，如果我在转角处看到大多数现代摄像头前面的红色LED灯圈，我可能会想它看起来多么像《2001：太空漫游》中的“哈尔”，然后继续走，在心里默默抱怨工业资本主义对我的隐私越来越多的侵犯。而现在，当我看到那个摄像头时，我立即开始评估移除它的最佳方式。

第二个转变是，这改变了我度过闲暇时间的传统模式。它让我对一周的其他部分有了更深的认识。每当我在工作中进行一项漫不经心的任务时，我的思想就会转移到那一周的行动目标上。这使得当时需要我全神贯注的工作成为了一种烦恼，但另一方面，那些我以前会觉得很烦的事，比如糟糕的司机、愚蠢的顾客，或者被打碎或丢失的财物，都无法在我的思想中获得立足点。我的思想中只有一个任务：摄像头。

[image]

摄像头 4、5和6

冬天开始了，把我推到了室内。和全国许多地方一样，我们度过了一个“极端”的冬天。我望着窗外，听着广播里暗示人们呆在家里，不要开车去任何地方。我期待着温暖的天气回来，这样我就又可以出去玩了。我看了乌克兰起义的视频。看到人们在外面和警察搏斗，用自制的弹弓把自制的燃烧弹投射到警察布下的路障上。路障是用雪做的……视频显示他们用麻布袋装满了雪，我意识到这是显而易见的事。

这些人在俄罗斯的冬天里日夜奋战，我突然感觉茅塞顿开！我需要推动自己。我突然想到：当民众们哈着热气窝在家里看网剧，警察忙着处理车祸和其他与天气有关的报警电话时，任何愿意冒着风雪出门干点什么的人都可以在这个城市里尽情奔跑。

当天晚上，我穿上保暖内衣，围巾，戴上大手套，在冬衣上又套上一

件大风衣，出门去测试我的假设。我想要的两个摄像头并不在主干道上，而是在一些酒吧后面的人流密集的停车场，平时那里的人很多，而且相当暴露。摄像头在一个窗台上，有点高，但也不是太高。我把自行车停在一家餐馆后面，蒙上了面罩，拿了一个牛奶箱，我以为站在箱子上就可以够到它了。我爬上牛奶箱，结果，差一点……我靠。

在希腊的摧毁摄像头行动。
https://youtu.be/AVcWKGWPto8

我每周细致的计划让我避免了在妥协的位置上不得不即兴发挥的压力。还有第三台比这高得多的摄像机，我在以后还有其他计划。如果有人在那晚看了那台摄像机的录像带，他将会看到以下内容：一个脸上蒙着头巾的人走近那对摄像机，把一个牛奶箱放在下面的地上，拿出一把剪线钳，伸手去够摄像机，没够到，就跳下来，疯狂地四处张望；接着跑遍了巷子里的每一家餐馆和酒吧，最后从其中一家餐馆后面拖出一个运货用的木质托盘，靠在墙上，爬到摄像头前，剪断了电线，并试图把第一台摄像头从支架上扭下来。那个摄像头仍然牢牢地贴在窗台上，我把脚蹬在摄像头下方的墙上，用全部上半身的力量来回扳动，直到摄像头终于松开，把我打得向后飞了出去。我爬起来，疯狂地四处张望，然后继续在另一个摄像头上尝试同样的动作。

在这种时刻，很难衡量时间，但我很确定，此时已经用了几分钟的时间，相比之下，我之前的动作肯定都是几秒钟的事。当我双脚紧贴着墙壁，双手拉扯的时候，我的目光落在了摄像头与支架连接处的一颗小螺丝上。回到第三个摄像头的视角。我停止了来回的拉扯，把脚放回木托盘上，冷静地拧开螺丝，再爬下来，把木托盘放回原处。然后走开了。

几天后，一场暴风雪袭来，让这座城市陷入瘫痪，而我又回到了外面，这一次是在一个曝光度很高的屋顶上，然而，在眼睛所能看到的地方，这里已经是一个被冰层覆盖的鬼城。而我就在那里，扶着一个卫星天线保持平衡，从上面踢着摄像头。我已经对接下来的汛期迫不及待了。

[image]

地点，地点，地点

除了简单地先找到容易下手的摄像头之外，还要想办法移除那些摄像头，这需要一个周密的计划。我已经决定，由于犯罪的性质，我应该避免自己出现在任何摄像头上。通过观看视频很容易确定犯罪的具体时间，而其他摄像头的主人很可能会配合警察帮助追踪那个特定时间前后有谁在这个区域。另外，如果在某个时候，这种行为模式被指定为政治性的—— 因为有人报警，或者是被精明的警察发现了—— 联邦的资金就会用来追捕我。这大大限制了我的活动范围和潜在目标清单。

我立刻想起了游击战的一条规则：每一次行动都应该让你有能力做一些以前做不到的事。正是考虑到这一点，我决定在我的镇子里建立 “隐私走廊”：可以让一个人在不被摄像机拍摄的情况下通过的路径。

[image]

我走过了一个不同的世界。这个孤独的秘密让我觉得自己是个超级英雄，或者是个恶棍。

今天，当我看到摄像机盯着我时，我仍然会感到那种最初的焦虑。

[image]

研究表明，当人类知道自己被监视时，他们的行为就会大不相同；他们会更努力地去符合社会规范，而不是脱颖而出。他们会变得焦虑和易怒，然而最终他们会在情绪上适应被监视，接受监视和焦虑为 “正常”。

我也一直都是这样的行为：眼睛向前看，不停地走，不自觉地权衡自己的一举一动会被如何解释。但现在不同了：最初的焦虑过后，我记得自己是在卧底，在策划，在回望。

在一个日益复杂的社会里，随着我们被要求越来越多的顺从，自我的空间变得越来越小。我指的并不是衣着风格、音乐品味、娱乐性用药等表面的表达形式，甚至不是宗教信仰和性偏好 —— 这些都可以被认为是能容忍的，只要它们的实践方式不破坏生产、消费或社会控制。

我的意思是，我们的行动自由，我们通过对世界采取行动来表达自己的自由，我们的自主性—— 这些都被大大地限制了。我们的头脑只能去适应这些有限的选择：就业、慈善、饥饿；或者买房、租房、无家可归；或者被观察、躲避、遵守和被忽视。

但有时我们会想起曾经还有另一组选择：自卫、进攻、毁灭。而我正是在这些选择中找到了尊严。当我现在对着摄像头行动时，我的笑容是真诚的，而不是被迫的。我知道我还会回来摧毁它们。

Maribor，对行车监视摄像机的攻击浪潮在2012年引起了斯洛文尼亚的全国起义。
https://youtu.be/YhymPYKKaNE

摄像头 7和8

我喜欢独自行动。这让人感觉安全，但也让人感觉很强大，专心致志想办法做事，执行那些需要认真判断的计划，并产生实际后果，而不需要别人来操作，只是相信自己。

所以我很难告诉你为什么我决定带另一个人上场。也许我认为我需要一个看家本领来完成一些我希望完成的更大胆的行动；也许我只是需要摆脱自己对整件事的束缚，获得一点看法。不管怎样，我决定拉巴特一起来做。我信任他，而且他也说过一些想采取类似行动的想法。我本来对他的想法装作不感兴趣的样子，当提到摄像头的话题时我总是这样做的。

他对我的邀请很兴奋。为了练习，我带他去了一个废弃的带状商场，那里的监视摄像机还完好无损，运作情况也很可疑。我想让他在紧张的环境之外学习动作，这样他就能在实际任务中专注于我们周围的环境，避免像我前几次外出那样的尴尬局面。

我们蒙面躲在树丛中，然后从第一个摄像头后面迅速接近。巴特踩在我的手上，我往上推。他把手放在墙上以稳定自己的身体。“现在用剪子把电线剪断，然后就拉着摄像机，看它会不会断。”

“不会断。”

“好吧，也许接头处有一颗手拧螺丝，看能不能拆下来？”

沉默……“搞定了！”他跳了下来。我们又拆掉了一个，然后回家了。

[image]

摄影头9

几天后，我带着巴特出去执行一个简单的任务，我一直在计划，但不得不一直推迟，因为酒吧的营业时间比我想象中要晚。一旦我终于找到了一个他们关门的晚上，任务就轻而易举了。

我们走近大楼时，一直用头巾蒙着脸，帽子放得很低，然后爬上靠后面的铁丝网，上了屋顶。我们在摄像机后面转了一圈，把摄像头蒙住，再剪断电线，把它塞进我的外套口袋里，爬下来，在摘掉手套和头巾之前离开了这个区域。

我们穿过一条后街的路线，向我家走去。“想不想再试一次？一个实验？”我问道。

“好啊，听起来不错。”这次我想要的摄像头在一个停车场的入口处，面朝水平方向，可以看到汽车进来的地方，也可以看到人行道。它被一个透明穹顶遮住，以隐藏它指向的方向。

我从上衣口袋里拿出一把锤子。“计划是这样的：我们绕一圈，从后面接近它，你留心观察，因为转动很稳定，我用锤子把罩子打碎，然后试着把摄像头扯出来，如果不行，我就用锤子砸它几下。然后我们就小跑着回到街对面的小区里。有什么异议或修改意见吗？”

“我加入。”

沟通我想做的事，并把它拿出来辩论，这感觉很奇怪。我觉得这是我的项目—— 而且事关重大，我准备好接受别人的意见了吗？我想，如果他说不，或者我们不能在一个计划上达成一致，我可以改天晚上再回来单独做。

我们按照计划的每一步进行，但当我挥动锤子时，摄像头转动了一下，我又挥了一下，它又偏离了。我绕过来想直接击中，它向我弹了回来。我们停了下来，耸了耸肩，尽力擦掉了那些宣布我们失败的痕迹，然后小跑着离开了。在一栋建筑后面摘下了面具。

[image]

新工具

我们讨论了如何处理穹顶的各种可能性。排除了放火的可能性，因为在美国对纵火行为的处罚非常重。我们还排除了仅仅在玻璃穹顶上涂油漆的可能性，因为那只是暂时的，我们希望摄像头被完全摧毁。与一些在这个问题上流传的主张如涂漆、剪断电线，甚至只是在镜头上粘上黑胶布的想法相反，我相信最好的办法就是彻底破坏它。

如果我们只是临时遮盖摄像头，它很快就会被修复，我们可能要反复返回重新做这件事。这就变成了模式行为：它给了敌人适应的机会，这就是你被抓的原因。

有一天晚上我们出去的时候，巴特向我汇报了他的最新调查情况。“我对穹顶做了一些研究，他们宣传说可以防破坏。有一个宣传视频，他们用汽车碾压它，并试图点燃它，都失败了。螺丝都需要专有的钻头来拆卸。但有一种工具可以用来处理穹顶的材料。它又长又细又锋利，在网上可以买到，所以我们可以用**Visa**礼品卡匿名购买 …… 但我还是不知道该把送货地点写成哪里。”

我们决定暂时搁置这个话题。与此同时，我一直在开发我自己的特殊工具，并很兴奋地在现场测试它。我在 Conglomo-Mart 的野营区偶然发现了一个叫 “突击队锯” 的小装置。它是几根粗铁丝缠绕在一起的，两端有布条指环。我把它塞进裤子里，把50英尺长的伞绳放进口

袋，然后走了出去。

[image]

返回：[image]如何摆脱手铐、绳索、束线带和布基胶带：反侦基础课 S06E04

回到家后，我从伞绳上剪下两段十二英尺长的线，把它们绑在“突击队锯”两端的环上，在一端加了一个沉重的钢链。我想象着自己把链子扔在摄像头上，调整好，让钢锯直接顶在上面，然后来回拉动绳子，锯开硬塑料支架。

我向巴特解释了这个工具，他很兴奋。“太牛了! 我一直在观察你上周跟我提到的一个地方，商场关门后不久，那边就没什么人了。直接够不着摄像头，但有这个新工具就很好办了。”

这是希腊。
https://youtu.be/YK891-tz0BA

摄像头 10、11、12和13

我们在商场关门后才接近商场，但时间选得足够早，因为这样可以让隔壁酒吧的音乐声淹没我们可能发出的任何声音。我们站在第一个摄像头的两边。我拿出一根绳子，把钢链扔到摄像机上。我的角度不对，它从墙上弹了回来，幸运的是巴特接住了它，没有撞到金属栏，否则会发出更大的声音。

我们重复了几次，直到我终于把钢链套在了摄像机上。我又放开一段绳索，直到锯子恰好挂在支架上面，然后我改变了计划。“让我们看看如果只是拉动它，会发生什么。”

“好，1、2、3！”我们俩用力一拉，锯子就断成了两半，摄像头又恢复了原状。

我的新玩具用错了，把它弄坏了，又没有备用方案。我想了一

下。“看看剩下的绳子够不够长，既然伞绳比较结实，那就直接扔过去把摄像头拽下来吧”。我之前以为支架不可能松软到可以用伞绳拉下来，所以我才会开发出精心设计的锯子装置。

但我错了。我们一拉，摄像头很容易就被拽下来了。巴特抓起摄像头，把它从还连接在建筑物上的电线中扯了出来。

“想做其他的还是收工？” 我问道。

“继续吧！” 现在，我已经掌握了使用绳索的窍门，我轻松地把它扔到了第二台摄像机上，它和第一台摄像机一样很容易被拉下来了。一般情况下，我这时就会回家了。出门，行动，回家，这是我的基本模式，虽然保守但安全。不过这时我才体会到与他人合作的真正价值：很有趣，而且你们会互相推动彼此的积极性。虽然有些任务看起来像是一个人的工作，但两个人的勇气和胆量可能会使事情更容易快速进行。我们没有回家，而是又去搞了两个屋顶上摄像头，我们很兴奋。

[image]

返回：[image]直接行动的关键在于协作，但协作的能力并非天生

 2004 希腊
https://youtu.be/ycc2ZMWoXhQ
 2007 希腊
https://youtu.be/LTTM0r79YKA

后来我们从小道消息中听说，那个商场的员工一直在闲聊，猜测摄像头发生了什么。我突然想到，每一个被我们毁掉摄像头的企业，可能都有一个老板很生气，甚至可能觉得受到了威胁，但也有员工肯定发现摄像头不见了，要么不在乎，要么觉得好笑。毫无疑问，当老板报警时，他们会回答：“是啊，我们最近有一连串这样的事。” 于是，谣言就这样传开了……

虽然不理智，但有时我还是为那些被我们毁掉摄像头的人感到难过。有些人是小企业主，他们可能想象着，不管是谁弄坏了他们的摄像头，以后可能会回来抢他们的东西或者做其他的事。

重要的是要记住，个别的人不需要出于恶意而成为极权主义系统的帮凶；事实上，这种系统几乎从来不是这样建立的。如果每个摄像头都是一个更大的监控系统的一部分，这个系统有效地监控着所有人，那么每个摄像头是谁放的这又有什么关系吗？如果录像被警察国家传唤，这些人中会有人反抗吗？甚至需要传票，他们就会像“好公民”一样把录像交出来吧？这有什么关系呢，因为大多数的CCTV都是连接到互联网上的，我们知道国家安全局和其他所有的政府机构都可以访问互联网上的几乎所有东西—— 所以，就意图和目的而言，这些都是国安局的摄像机，每个摄像头的主人只是在监控封建体系中打理自己的小地盘而已。

2012年，在斯洛文尼亚马里博尔，活动家用汽车拉下交通监控摄像头。
https://youtu.be/fWJbGT_oIDc

摄像头14、15、16、17、18

这时候我对与第二个人合作的任何顾虑都消失了。巴特已经开始熟练行动，做研究、侦察，并且让我有点紧张 —— 在我们做完其他四台摄像头的同一周，他自己就完成了五台摄像头的工作。

“我从来没有说过你不应该自己做这件事，但可以考虑放慢一点速度，我们要足够低调，以保证能够继续做这件事。如果我们想有所斩获的话，就肯定要去努力，但在行动过程中留下不规则的静默时间，会大大增加我们不被抓住的机会。我不想耽误任何人砸烂世界上所有的摄像头，但要把握好自己的节奏，这样我们才能长久地投入其中。”

我也跟他说了我的个人政策，在我要攻击摄像头的日子里，我不会到处乱跑，所以在整个区域里不会有我的记录。“我知道对于每一个单独的轻罪破坏行为来说，这似乎有点过于谨慎了，但如果在某个时候，警察发现了我们的行动模式，并给它贴上了某种行动主义的标签，他们就会开始追踪我们。低调以保持安全不会让我们后悔的。”

[image] 香港

摄像头 19、20、21、22

我决心继续研究所谓的防破坏摄像头，于是我去 Lowe’s 找了一把锤子和我能找到的最大的凿子。

我们蹲在街对面一家关门的企业后面，蒙上面罩，仔细检查了工具，戴上手套。这装束是冬天看起来很普通的事，在炎热潮湿的夏夜里却显得异常荒唐。我们在稀稀疏疏的车流中等待着，那些零散的人还在从关门的酒吧回家的路上。那个时候出门的只有醉汉、出租车、警察和罪犯。

我们冲到街对面的目标处。我把凿子的尖端对准穹顶，用锤子反复敲打。我一遍又一遍地挥动着，至少有十几次。它贴着的电箱每打一下都会发出巨大的低沉的轰鸣声；穹顶表面出现了一簇深深的凹印，但凿子却无法穿过它达到摄像头本身。

“有汽车！” 巴特阶段性地低声说了一句，我们小跑着进入安全距离的地段。

“没事，该实施B计划了。” 我说，从包里掏出一罐黑色的喷漆，向摄像机方向慢跑回去。

“一切正常。” 巴特说，他负责放哨，上下打量着街道。我在穹顶上喷了一层厚厚的油漆，也在穹顶周围也喷了漆，让油漆滴落下来，任何一个路人都能从远处看出这个摄像头已经失明了。我们又去把城对面的另一个摄像头喷了一遍。

“我们会一直关注这些被喷漆的摄像头，看看它们被洗干净需要多长时间，了解清洗过程中是否会刮花穹顶。这可能会成为我们只是在时间敏感的问题上采取的行动方案，比如游行什么的，但这不可能是一个永久的解决办法。”

我们很兴奋，于是走近一家餐厅，餐厅里有两个摄像头对着人行道，

那是他们所谓的财产边界。我们开始比较自然地协调行动。我们几乎没有商量就走近了，我看了看街道两边—— “安全！” 我们俩跳起来，抓起一个摄像头，然后扭动。然后从来时的路跑了出去，跑进了一个居民区，确定安全后再摘下面具，脱掉了外衣，走进夜色中。

示威者在2012年摧毁斯洛文尼亚马里博尔的监控摄像机，https://youtu.be/WV_YBEQcfrU

侦查

当 Lisa 指出商场外的两台摄像机时，我一直在想它们。每次经过它们时，我看的不仅仅是想知道如何把它们拆下来，而是想看看这个空间的活动范围如何。什么时间段内此地是活跃的？什么时间段不活跃？

一天晚上，我有一些多余的时间，决定可以在商场外面坐一会。我大部分时间都坐在离得很远的长椅上，但我预计在某些时候必须靠近摄像头，查看从长椅上看不到的巷子，所以我里面穿了不显眼的衣服，外面是一件明黄色的外套。明黄色夹克是我从学习识别心理学中悟出的一个窍门—— 人们只会记住你最明显的特征，比如你的亮色衬衫或俗气的鞋子，然后再在记忆中编造其他的部分。后来，我把这一招延伸开，在侦查的时候，我的走路方式和平常不一样。

[image]

返回：[image]匿名着装 ；[image]生物特征隐藏

我坐在商场外观察。三十分钟内，连摄像头附近都没有人走动。我换了个位置，到巷子里观察。没有人。很奇怪。我在长椅上多坐了一会儿就回家了。为了防止我侦察的那个晚上是个例外，我第二天晚上又回来了。那天是周五，摄像头就在一家酒吧旁边，所以如果这个时候没有人经过，我可以确定这不是一个偶然事件。我在酒吧关门前一小时到达。同样，没有一个人经过。我观察了大约二十分钟，足够长的时间来确定这个地方会是一个简单的行动地点。

太容易了，也很好玩。

华盛顿特区
https://youtu.be/NnQi2NHv4hg
[image]

这篇文章的最后写着："所有行动和文本敬献给 Jeremy Hammond"。**Jeremy Hammond** 是匿名者组织成员，天才计算机程序员、活动家、和吹哨人。他因泄露私人情报公司 **Strategic Forecasting，Inc.**（**Stratfor**）的秘密而被判入狱十年。这是他的认罪协议所允许的最高刑期。

[image]
[image]

在街上保持安全：街头实战指南S05E12

[image] 关键词	准备工作 匿名着装 协调 街头 街头战术 逮捕
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月15日 9:00 (GMT+8)
[image] Description	行动安全性

关于，如果您在街头，至少应该知道的一些事情。

- Table of Contents

  1、穿着
  2、有备而来
  3、在街上
  4、之后

[image] [image] [image]

上图是美国反抗者给队友的建议。

本集是一份非常简短的指南，更详细地解释上述这些图片。如果您要上街，不论是大规模的群体运动还是小团体的行动，这里是您需要了解的基本知识。

1、穿着

[image]

返回：[image]匿名着装

穿多层的衣服，即使是在炎热的天气里：外面的一件衣服进入行动区域，让您看起来就像个普通人，完全融入人群；里面的另一件衣服用于行动本身。

脱衣服会比换衣服或穿衣服更快，更有隐蔽性，于是，如果您能穿第**3**层衣服的话，可以帮助您在退出时再次以与进入该区域不同的样貌融入人群中（这是假设镇压者搜索了所有进入该地区的人的监视录像，这种可能性也许很高）。

您的身体上有可见的穿孔吗？耳朵、鼻子、下巴等部位，将饰品全部取出来；掩盖所有可见的纹身。您的身上有疤痕吗？明显的痣呢？胎记？必需掩盖起来，要掩盖得很自然，掩盖物绝对不能让您脱颖而出。

[image]

有些抗议者穿着相同的衣服 —— 黑色连帽运动衫、黑色长裤和口罩 —— 为了让人无法分辨。如果您的亲密团队也准备这样做，请确保您的衣服没有任何可识别性特征。请记住，您的鞋子或背包也可以识别您的身份。

[image]

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

如果您戴着口罩，戴上口罩的时候需要躲避一切摄像机或警察 —— 事先侦查很重要，并且在行动中要一直戴着它。把头发完全遮住，您的头发颜色和发型特征都可以用来识别您。

面罩很重要，不仅是避免被身份识别的问题，最重要的是它可以保命，在这里看到选择面罩和防护功能的具体介绍。但如果没有任何面

罩，防护功能就无法达成了，而您依旧可以实现免追踪功能。只需要一件T恤衫就可以—— 将T恤套在头上，将领子部位盖过眼睛，将袖子紧紧地绑在脑后，衬衫的其他部分遮住头部和肩膀。根据透光程度，考虑是否在眼睛部位剪两个孔。

[image]

请注意，警察很可能会将目标锁定在孤立的蒙面人身上，所以，在到达安全的地方之前，您和队友一定要一起换衣服，然后散开。

护目镜可以保护您的眼睛不受化学武器的伤害；太阳镜可以使您的身份可辨识度降低。

小心隐形眼镜会将化学武器困在眼睛上！尽可能不要佩戴隐形眼镜。

如果您很有可能被催泪弹或胡椒喷雾击中，浸泡在苹果醋中的头巾可能会帮助您更好地呼吸。戴布手套（就是那种礼仪手套），因为乳胶上会粘上指纹，皮手套上也会留下您自己的指纹。

[image]

返回：[image]DNA最小化方案 ；[image]手套

2、有备而来

您可以带上水、急救用品、横幅、旗帜、鼓、哨子、扩音器、音响系统、可作为盾牌的标志、贴纸、喷漆、信号弹、火把、装满油漆的圣诞树饰品、鞭炮、锤子或警察扫描仪等等。在这里看到关于您应该带什么和最好不要带什么。

[image]

返回：[image]您需要真正的“自己人”：整体安全S01E09 - 进入战斗状态

提前用酒精湿巾擦拭任何您可能在街上丢掉的东西，把指纹弄掉。

考虑用一个临时手机代替您常用的手机。

请记住，您的通话记录和短信可以在任何与您的名字相连的手机上追踪到您；如果警察抓到你，肯定会检查这些 —— 至少检查这些。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

返回：[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

确保您知道一个可靠的电话号码，如果您被逮捕或与朋友走散并需要帮助，您可以拨打这个号码。如果无法确定可以牢记，就用不容易褪色的记号笔写在身上隐蔽的部位。

使用亲密团队系统与您信任的朋友们保持联系。提前谈好你们要做什么以及如何沟通。

提前确定目标、材料、危险区域和逃生路线。提前计划好如何以及在哪里可以分散。

[image]

返回：周密的行动计划

3、在街上

尽可能确保和队友呆在一起。不要让人群太过分散，前后左右之间要携带信息—— 确保在中间隐蔽位置的相对弱势的队友能及时获得周

边局势准确的信息。不是咬耳朵游戏哦，是要准确的局势观测。这意味着您的团队有事先确立的角色分配，关于如何分配角色，见下面：

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

骑自行车的朋友可以让您了解更大范围内附近的最新情况。当然，这是侦察员角色。

[image]

返回：[image]自行车接力

一旦在侦察员没有通报的情况下警察就出现了，要向侦察员队友说明，他们没有尽责。不用担心，您的强硬态度和保护彼此的意愿是您的通行证。而队友不应该生气，这也是安全文化的一部分。

如果您是侦察员，要知道，警察会虚张声势，会撒谎，但您也许可以通过他们看起来的物质准备来预测他们的下一步行为。

不要让警察进入人群。沿着密集人群的两侧举起横幅，如果有必要的话，可以手拉手。如果警察想抓人，就挡住他们的去路。

[image]

保持移动，这样警察就没有机会把你们抓起来。

如果您看到警察封锁了前面的一条街道，在他们包围和困住你们之前要快速移动。让警察去猜测，为自己赢得时间。记得，警察是官僚主义的，他们的行动肯定比反抗者队伍更慢一点。

[image]

4、之后

如果警察要和您说话，不要理睬他们，除非他们明确指出您正在被拘留或逮捕。如果他们抓住您，不要反抗，除非您确信您能逃脱；反抗会使您受到更严重的指控。

如果您被逮捕，请行使您保持沉默的权利。无论警察说什么，除了您的姓名和地址外，不要回答其他问题。永远不要告诉警察关于其他人的任何事，即使是看起来微不足道的小事，都不要说。

[image]

返回：[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

不要在 Facebook、Twitter 或任何其他网站上发布任何您不会直接向警方展示的内容。不要吹嘘自己参与过的任何激进行动，也不要描述他人的行为。只与您信任的人在安全的环境中谈论发生的事。

[image]

返回：[image]信息最小化原则

企业媒体会重复警察的谎言。政客们会试图诋毁行动者，或者让您在无休止的上访中浪费时间。不要让他们恐吓您或阻挠您的想象力。

行动者的力量来自于我们自己的勇气、梦想，以及与他人建立的联系。

[image]
[image]

和媒体说话时如何避免陷阱：街头实战指南 S05E13

[image] 关键词	信息民主化 宣传 职业媒体 街头
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image] 创建时间	2025年1月16日
[image] **Description**	行动安全性

请随时记得，职业媒体所依赖的经济体系往往正是您致力于颠覆的旧政权的命脉。

- Table of Contents

在与媒体交谈之前
1、考虑是否有另一个人或团体更适合就某个问题发表公开声明。
2、考虑记者、编辑和他们的听众将如何看待您的行动。
3、考虑到目前面临刑事指控的活动家或将来可能面临刑事指控的其他人的风险。
4、事先确立明确的目标。
5、编写您的谈话要点，并练习简明扼要地陈述。
6、明确您将与之交谈的媒体的议程。
7、事先考虑您对这个记者有什么影响力？您对这个报道出现的地点有什么影响力？
8、当您与记者交谈时，事先就他们如何识别您以及他们将发布哪些信息，达成协议。
一位富有同情心的记者给活动家的建议
1、在任何时候都要直接。
2、如果您挑战记者，不要把记者逼到墙角。

3、不要侮辱记者的智商。
4、要非常具体。
5、不要指望所有这些原始信息都能被写进报道。
6、保持接触。
7、要有极低的期望。
8、找出那个记者的编辑是谁。

[image]

[image]

返回：

延伸：https://iyouport.substack.com/p/2b6

反抗者长期以来一直对媒体本身的功能持批评态度。然而，要避免新闻报道并不总是可能的；在信息时代，要么有强大的自传，要么被杜撰。

当您为追求社会变革而采取有效行动时，媒体机构将寻求在公众面前代表您—— 除非您能扰乱他们的叙述，否则全世界的大多数围观者都将通过那些媒体的眼睛来看待您的行动。

这也是为什么全世界很多抗议活动都遭到了严重的误解。

延伸：https://iyouport.substack.com/p/cf8?utm_source=publication-search

您的反抗行动越是对变革有效，您被抹黑歪曲的程度就会越大，这是绝对成正比的，现在您明白为什么直接行动被抹黑为 “恐怖分子”了？正因为直接行动不再依赖统治阶级的恩赐，架空了他们的权力。

不论是中国的官方媒体还是美国的企业媒体，都不是一个中立的空间，不是那种您可以像与同事和邻居直接对话那样提出想法。媒体是一个战略要地，当局在上面为自己定位，操纵叙事，使武力的使用合

法化。

走到企业媒体的镜头前就是进入了一个决心操纵反抗者的形象来对付反抗者的阶级所控制的敌对领土上。如果您让媒体把您描述成暴力的、异类的、或极端的 —— 无论您为您的反抗战略或变革思想提出多么有力的论据—— 最终的结果都将是当局更有信心加强对您的攻击。

当与媒体打交道时，反抗者首先不能想象那些媒体会如实地阐述反抗者的思想；您必须通过自己的渠道来完成这一任务，这就是为什么反抗运动应该有自己的网站和发言人。

充其量，您可以利用媒体的出现来引导人们进入您的信息输送渠道，就像那个坚持只在显示自己的网址的横幅前接受采访的组织那样。

请记得，您正在进行一场微妙的立场之战，在这场战争中，您的目标是防止当局驱散您的反抗运动的可能支持者队伍，并破坏当局使镇压暴力合法化的叙述。您必须始终平衡在合法性和能见度方面可能获得的收益与使自己成为更引人注目的目标之间的风险。

不应该忘记SHAC运动的例子，它试图关闭一家动物试验公司。起初，该运动取得了很大的进展，随着媒体对其组织效果的宣传，势头越来越猛 —— 然而，最终，执法部门能够利用这种威胁性的形象，策划了一场镇压，将许多人送进监狱多年。

对此，本集提供以下建议，希望能帮助您在与媒体的互动中保持安全。

[image]

在与媒体交谈之前

1、考虑是否有另一个人或团体更适合就某个问题发表公开声明。

在接受采访之前，请咨询可能会受到您所说的话影响的任何其他人，以获得他们的反馈，修正您的表达方式。

2、考虑记者、编辑和他们的听众将如何看待您的行动。

以及，您是传达这一信息的最佳人选吗？

延伸：https://iyouport.substack.com/p/28?utm_source=publication-search

3、考虑到目前面临刑事指控的活动家或将来可能面临刑事指控的其他人的风险。

请记得，即使是最无害的声明也会被大局恶意操纵，以抹黑和诋毁活动家，特别是那些已经面临刑事指控的活动家。

您在新闻采访中所说的每一个字都可以被利用于：

- 在刑事诉讼中
- 起诉被采访者或其他与公开声明有关的人
- 传唤被采访者为检方作证，以对抗他或她的队友和其他活动家。

4、事先确立明确的目标。

在这个媒体上出现，您要达到哪些具体的收益？

您将如何实现这些收益？

例如，如果您试图吸引更多的人加入即将举行的示威活动，在可能加入您的人阅读的报纸上获得报道可能是有意义的，但是，在主要由希望看到这类抗议活动被压制的反动分子喜欢阅读的报纸上出现可能就没有意义了。

5、编写您的谈话要点，并练习简明扼要地陈述。

记者往往会问一些诱导性的或敌对性的问题，以诱使您提供他们需要的材料来讲述一个预先被确定的故事。如果您与媒体打交道的经验有限，请先与那些有更多经验的人交谈一下。

6、明确您将与之交谈的媒体的议程。

他们希望达到什么目的？他们利用的基本语话条款是什么？您怎样才能扰乱他们所宣传的叙述？

7、事先考虑您对这个记者有什么影响力？您对这个报道出现的地点有什么影响力？

如果您没有足够的公信力基础 —— 也就是说不够著名，那就要非常谨慎，因为您在公众眼中犹如一块白板，媒体可以随意对您涂抹。不要给他们这样的机会。

8、当您与记者交谈时，事先就他们如何识别您以及他们将发布哪些信息，达成协议。

请记得：要强调您 不代表某个政治派别，也不充当 “运动的领导者” 。

如果您使用假名，要注意确保没有人能够查出您的合法身份；警察经常强迫记者透露媒体发言人的“真实身份”，以此来危害和诋毁活动家。

[image]

一位富有同情心的记者给活动家的建议

1、在任何时候都要直接。

拿着录音机的人认为您很可疑。他认为您已经成为您自己制造的智力陷阱的受害者：认为您无法欣赏细微差别或认同您的敌人。在他看来，他的工作就是介绍您的信息，而不被吸纳为您的反抗队友。

他会问您很多很多问题（比如谁在资助这个组织？你们不都是大学毕业生吗？你们有没有考虑过上访？我可以看看你们的成员名单吗？……）；您应该在适当的时候完整地回答他们。如果您的组织是松散协调的，那么直言不讳地承认无中心要比把自己说成是一个稳定的联盟或单一的实体更重要，因为事实并非如此。

没有人喜欢被审问，但如果能记住觉得您没有保留什么，那对您来说就更好了。

2、如果您挑战记者，不要把记者逼到墙角。

记者不喜欢被提醒他们不知道什么。因此，如果您说一大堆专业术语或引用晦涩的文字，就会让记者感到自己很无知、暴露和愤怒。记者会把您描绘成冷漠的精英分子，在重要的事情上演戏。

如果记者在你们的谈话中得出了不恰当的结论，澄清您所说的内容比反驳他们要好得多。

如果记者继续歪曲您的说法，在报道发表后给他们的办公室打电话，警告他们的编辑其员工中有一个捏造者。

记住这个词——“捏造者”，也就是说，骗子。这三个音节会让编辑们惊出一身冷汗。

3、不要侮辱记者的智商。

这并不是说这个记者不聪明。很少有记者不表现出至少是基本的智力，因为他们的工作取决于调查。拍马屁会让您无功而返，因为记者不喜欢被吹嘘。

但礼貌和细心是值得赞赏的，因为这往往是一份累人的工作，而报酬却很低。

如果您以尊重和开放的态度对待记者，他甚至可能重新考虑他的态度。

4、要非常具体。

记者要的是事实。您希望事情有所改变这就是事实。

在您的采访中，详细解释您打算做什么，如何做，以及为什么。

如果这涉及到当局所认为的非法活动，请非常清楚地描述您行动的动机。

延伸：https://iyouport.substack.com/p/ad0?utm_source=publication-search

5、不要指望所有这些原始信息都能被写进报道。

但是，您给记者的信息越多，记者就越需要填满他们的专栏、字数或广播时间 —— 而所有这些都将来自于您的一方。也就是说，尽可能用您的语言占满他们的版面。

记住，您接受采访是在给记者访问权，您对抗的当权者则不会。这对您来说是一个优势。

6、保持接触。

与您打交道的记者可能会想问一些后续问题。如果您不在身边回答他们，他们就会对您的情况做出推断和假设。如果您向他的编辑抱怨，记者将能够可信地辩称，您没有接听电话或回复电子邮件，而记者有一个截止日期要完成 ……

记者将赢得这场争论。不要让他们得逞。

7、要有极低的期望。

记者的倾向是，只刊登您的故事中必要的内容，以便记者回到办公室可以投入到更有趣的任务中。这一点对年轻记者来说，甚至比年长的记者更真实：年轻记者在更好的工作或更好的局面出现之前，一直在计时，而您那一文不名的革命性的滑稽动作就是他们的时钟的刻度。

遵循上述指示，您的信息就会通过这种媒介传播出去，只要有可能。

当然，您可以选择使用您自己在网站或其他地方的账户来补充您在主流媒体上被削减的表述，但那始终是您的领域，不是记者的，大众会将此理解为 “主观”。

8、找出那个记者的编辑是谁。

这很狡猾，也很有效果。

问那个记者在哪个部门工作？记者会把这理解为您作为新闻联络人勤奋工作的标志，充其量是对记者重要性的礼貌性认可。实际上，这是一个为您所用的工具。

如果您对记者的报道不满意，请联该记者的编辑，并逐条说明您的不满。

一些注意事项：不要咆哮，要准备好具体的事实性错误或马虎的问题。正是在这一领域，电话或电子邮件另一端的编辑将准备采取行动—— 要么进行更正，要么指派另一名记者来报道您并对该记者进行约束。如果您试图纠正解释，编辑只会认为您是个怪人，并为记者撑腰。

[image]
[image]

加固横幅和盾牌的制作和使用方法：示威参与者指南S05E14

[image] 关键词	协作 团队 护盾 横幅 街头 街头战术
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月17日
[image] **Description**	行动安全性

要成为真正的革命，起义需要无政府主义理念和社会组织形式。

列出清晰的短期优先事项清单，以充分把握这些转瞬即逝的起义时刻。

切忌贪多求全。如果街头行动间隙尚有余力，请专注推进单一项目：制作盾牌
展社交媒体倡议、分发传单、组织避开人群的小规模邀请式行动，或策划大型
动。

可通过口耳相传、传单或社交媒体召集社区集会，创造讨论理念与策略的契机
人们在现实中相聚的场合 —— 这些空间能让我们分享观点、传播文献，并建
完全能够通过自我组织来安排整个生活，无需政府、无需任何等级制度的压迫

- Table of Contents

  完善防御工具
  盾牌和加固横幅
  盾牌
  金属加固横幅设计
  使用加固横幅

附录：为起义做好准备
起义
亲密
自主组织

[image]

本指南探讨如何制作加固横幅，使其在示威活动中充当移动盾墙。

需明确的是，我们绝不鼓励任何人利用横幅或盾牌从事非法活动。这些设计仅为满足历史学者的研究需求。

完善防御工具

本市的无政府主义者历经数月改进加固横幅的设计。我们使用这些横幅抵御警察暴力。在数十人协同行动的大型抗议中，这些横幅常在攻防两端发挥作用。

最初我们采用木质框架结构：选用轻便坚固的木料，配以金属握柄确保稳固，再将防水布覆盖其上。框架比较结实，三人即可搬运。然而，即便采用轻质木材并多次尝试更轻的木材，整体设计仍然过于笨重。此外，有外地同志指出横幅在行动进出时过于显眼 —— 在他所在的地区，横幅可折叠收纳。另一问题在于，木架覆盖的帆布极易被脚踢或警棍击穿。

我们的新设计经过测试效果令人满意，具有四大核心优势：**1**）轻便；**2**）低成本 ；**3**）可折叠； **4**）结构紧密。

在收到众多城市的行动者对新设计的热情响应后，我们编写了这份指南。



盾牌和加固横幅

盾牌与加固横幅可实现多种功能：

1、抵御橡皮子弹、水炮、警棍、胡椒喷雾，以及冲撞或拳击的攻击。

2、保护盾牌后方的行动者，无论是投掷石块、使用油漆灭火器等工具的行动者，还是单纯需要庇护或协助的人员。

3、遮蔽盾牌后方的行动，包括更换衣服、或准备工具。

4、作为坚固屏障抵御对手，避免笨拙危险的肢体缠斗。

5、发挥威慑作用，令敌方心生恐惧或疑虑，尤其是当持盾者人数众多时。

6、充当诱饵，吸引警方注意力 —— 尽管盾牌本身风险不高，却能使同伴在警方分神时快速采取行动。同理，警方经常首先专注于夺取盾牌或标语，而非逮捕人员。与其拖走战友，不如让警察去抢去这些胶带和塑料制品。

相较于加固横幅，盾牌更轻便、且易于制作；持盾者能获得更强的机动性和临场应变力。持盾者可随时弃盾奔跑，自主决策。在需要灵活机动的场合，盾牌可能是最佳选择。

[image] 缅甸的盾墙。



加固横幅的核心价值在于其体量以及它们在物理上和组织上的力量。由于需多人共同持举，这类横幅更难被撕毁，从而提供了更强的防护。警察无法轻易扑倒横幅另一侧的抗议者。加固横幅不仅能阻挡单个警察，更能阻止多名警员协同冲撞人群的状况。

由此，人群得以与警方形成力量平衡，划定明确的控制区域。

我们在本地的抗议活动中目睹过十余名同志共同撑起一面加固横幅，与对面十余名警察展开力量较量—— 当警方试图冲击人群时，横幅后方不断抛掷油漆、石块和烟火。组织层面而言，多人持举横幅的阵势能凝聚人群共识，形成防御与行动的焦点。这尤其能阻断警方以威慑手段瓦解群体的企图 —— 当警力不足以通过其他方式实现瓦解时，此法尤为有效。

盾牌

最终选择盾牌还是加固横幅，取决于您采取对称还是不对称的冲突策略。—— 您的目标是通过正面较量争夺或守住阵地？还是更重视机动性和必要时脱离人群的能力？失去突袭优势后，需要维持正面对抗多久？

[image]

加固横幅能提供更强的防警力保护，但固守阵地的过程中易暴露其他弱点。

答案取决于行动性质和地点：若为普通起义，盾牌更优；若属集中进攻或大规模人群防御，加固横幅则更合适。

[image] 图示I

在图示I 中，您可以看到另一组设计的防护盾，其采用纸板作为缓冲层，结合切割后的垃圾桶部件，并使用绳索、软管或自行车内胎进行固定。我们对第二层塑料（垃圾桶盖）的功能有些困惑，建议将纸板作为手臂支撑的缓冲层—— 否则警棍等强力冲击可能击穿塑料，导致手部严重受伤。塑料表面通常无法承受任何类型的直接冲击。

同样建议用胶带包裹所有锐利边缘，以防跌落时造成误伤。我们以前用垃圾桶部件制作盾牌时，通过厚层胶带包裹使纸板牢固粘合，握柄也用胶带缠住。总之，日常废弃物就能轻松组装出盾牌。

[image] 2025年6月抗议ICE暴力镇压示威活动中使用的临时盾牌。

> 不同设计的盾牌适用于不同场景。如同雨伞和吹叶机，盾牌在群体协作时能实现单枪匹马无法完成的任务。若要构筑盾墙，理想状态下盾牌应足够覆盖全身。但盾牌越大，重量越重、体积越大、携带越困难。小型盾牌则更轻便，更易潜入对抗区域。许多人在承担盾墙维护之外的其他职责时，仍随身携带小型盾牌。哪怕仅有微弱防护，也曾挽救过很多人免于重伤，并赋予他们坚守阵地的信心 —— 若无此防护，这些阵地恐难守住。
>
> 波特兰常见的盾牌制作法是将塑料桶垂直切割成三至四个有弧度的矩形，保留桶顶桶底的圆形部分制作小型盾牌。
>
> 构建盾墙时，盾牌需略微重叠排列，因“墙体”上任何细微空隙都可能形成破绽。因此针对此用途，胶合板可能比大塑料桶更具优势。
>
> —— 波特兰抗议中的工具与战术

2020年7月，奥克兰参与乔治·弗洛伊德抗议运动的第58天：一场声援波特兰民众抵抗联邦镇压的活动中，抗议者筑起盾牌墙。影像由莎拉·贝尔·林拍摄。
https://vimeo.com/1093627931?fl=pl&fe=sh

金属加固横幅设计

重要提示：下面的图示II 仅展示了两段式的加固横幅，但我们建议采用三段式设计，其覆盖范围更广。每段横幅由一人持握；如图示II 所示，每段均配有左右手专用握柄。各段通过扎带沿着连接边全长固定，可实现相互折叠收纳。

建议采用三段式横幅设计，以便由三人协同持举。

[image] 图示II

[image] 指纹 ：建议您在制作横幅过程中接触相关材料以及处理横幅本身时佩戴[image]手套 。制作加固型横幅虽不违法，但出于多种原因，建议您尽可能少地与之产生关联。 BACK [image]DNA最小化方案

[image] 图示III

接下来将逐一诠释上面图示III中的7个元素。

1.) 金属：我们通过切割临时施工围栏获得金属框架。可使用断线钳操作。所需金属材质应坚固轻便 —— 而非链式围栏那种脆弱易弯的类型。切割尺寸建议为高约3.5英尺（约1.07米）、宽约2.5英尺（约0.76米）。测量时需确保：蹲伏时金属板能完全覆盖身体；直立时可将头部藏于金属板后方，同时仍能遮挡部分腿部。

[image] 这种金属围栏比较合适

2.) 波纹塑料板：我们选用坚固且具有缓冲性能的波纹塑料板，此类材料常用于制作庭院标牌。坚固的硬纸板也能达到相同效果。无论采用何种材料，其长度和高度都应大于金属部件。这样在将硬纸板固定于金属板后方时，可避免金属部件撞击身体。

[image] 波纹塑料板

3.) 束线带：使用束线带将波纹塑料板或硬纸板固定在金属板上。确保第二层完全紧贴金属板。

4.) 手柄：

如图IV所示，手柄需要由三部分组成：a) 海绵 b) 束线带 c) 胶带。海绵应选用厚实且具有缓冲性能的材质，手掌置于海绵上时应感到舒适，并能有效隔绝冲击力。在海绵上方和下方于纸板上各开一个孔，使海绵能通过扎带完全固定在金属上。反复缠绕胶带直至形成牢固的手柄。握住它试试看，确保手掌能置于胶带手柄与海绵之间。

[image] 图示IV

制作两个手柄：一个较高，另一个位于其正下方，两者均水平居中。

现在您应该能够提起横幅了。

5.) 包裹边缘：用多层胶带包裹金属边缘使其柔软，以防横幅撞到您或他人。

重复上述步骤三次，形成横幅的三段结构。

6.) 束线带连接三段结构：沿相邻边缘添加束线带将三段连接。例如双人横幅示意图中，左右两段通过贯穿中部的束线带连接。这些束线带将作为铰链，实现横幅折叠的功能。

7.) 涂绘防水布：将长条防水布覆盖于三段横幅正面，将边缘向后折叠包裹至横幅背面，用扎带牢固固定。防水布是加固横幅的核心部件。在防水布上绘制标语或图案。如果使用喷漆可简化操作，建议配合模板使用，以获得更佳效果。

[image] 图示V

使用加固横幅

组建一支负责持举横幅的小组。由于该小组成员将在任何冲突中占据前线阵地，所以每名成员都应配备头盔、护目镜、面罩和手套。并且需要 提前商定 目标和计划，包括彼此间的具体协作承诺、及各类情境的应急预案。

建立快速沟通与决策的 暗号 至关重要，以便必要时能迅捷行动。 行动前务必演练确认 。

再组建横幅队的护卫支援队。其队员可配备各类防护工具（包括雨伞）以保护横幅队成员。我们曾目睹人群在横幅后方使用激光笔、投掷物、装满颜料的灭火器等工具。

横幅边缘是最脆弱的部位。可通过以下方式应对：在横幅两侧部署持

盾牌和雨伞的人群，或保持一侧有墙体作为屏障。务必避免陷入包围 —— 横幅的主要安全保障在于身后控制区域的人群，必要时可提供后援或撤离。若警方逼近，可能试图抓住横幅的上下边缘进行拉扯。大家应该保持机动性并阻止警方的拉扯行动。

可事先与可信赖的其他团队低调协调，告知对方您携带的是加固横幅。讨论双方行动计划的衔接方式。

需提前明确行动目标，商定横幅的部署时间与地点。为保持突袭效果，可能需要将折叠后的横幅伪装成抗议标语堆等普通物品，偷偷运入行动区域。

如果警方提前发现了加固横幅，未必允许其进入潜在冲突区。在极端困难的条件下，可提前将横幅运至相对安全的地点（如闲置工地，隐蔽存放），或待游行开始后再携横幅加入队伍 —— 此时警方往往忙于应对突发状况。

此款横幅设计轻便，可通过自行车运输。 BACK [image]自行车接力

其他战略考量包括确定横幅在行动区域的部署位置，尤其当您期待它同时具有干扰和防御两种功能时。

必要时请果断丢弃横幅。我们通常在行动结束后立即撤离时丢弃横幅。横幅是工具而非需永久持有的财产。横幅不等同于人——保护人员安全始终优先于保护工具。理想状态是让警方无法回收横幅以研究其构造或进行取证分析，但为此冒着被捕或暴露身份的风险绝不值得。

世界各地的抗争者曾尝试在金属购物车等装置上搭建移动式横幅，既可充当移动路障，也能作为冲撞工具。

我们认为加固横幅无法替代固定路障的建设 —— 后者能在特定区域为更大群体提供同等防护。

[image]

附录：为起义做好准备

我们目睹了2019年智利和香港起义中盾牌的部署，见证了2020年乔治·弗洛伊德抗议期间波特兰等城市的盾牌运用，更在亚特兰大森林保卫战等斗争中看到加固横幅的运用。

当下，动荡正在加剧。我们需要有更多同志能具备自己动手的能力。

以下是为起义准备的若干鼓励之言。

起义

起义是针对权威力量的战斗性直接行动。只要此类街头行动对您可行，请全力以赴。

在我们的城市，动荡时刻人们常沉迷于写作项目、社交媒体和大型会议，却错失了制定街头行动计划或打击基础设施的良机。

起义时刻必须放下一切。

这是我们毕生等待的时刻。

让我们策划突破常规的抵抗行动，展现我们能走多远，以及我们对此刻的重视程度。

亲密

专注于与您已建立深度信任的小团队的协作。这些应是与您理念契合、价值观相通、风险承受度相当的小伙伴。

通过会面制定计划并做好准备，确保行动时充满信心且协调一致 —— 尤其在可能出现变数的场合。

最基础的形式可以是：清晨快速会晤，午间共同准备工具，夜间前往抗议现场。

保持团结，彼此照应。不惜一切代价保护战友。在此， 爱是战斗力 ，不要吝惜展现爱，在行动前、中、后都要向亲密队友展现您的关怀。

自主组织

要成为真正的革命，起义需要无政府主义理念和社会组织形式。

列出清晰的短期优先事项清单，以充分把握这些转瞬即逝的起义时刻。

切忌贪多求全。如果街头行动间隙尚有余力，请专注推进单一项目：制作盾牌等装备、开展社交媒体倡议、分发传单、组织避开人群的小规模邀请式行动，或策划大型团体联合行动。

可通过口耳相传、传单或社交媒体召集社区集会，创造讨论理念与策略的契机。

必须培育人在现实中相聚的场合 —— 这些空间能让我们分享观点、传播文献，并建立信心：我们完全能通过自我组织来安排整个生活，无需政府、无需任何等级制度的压迫。

[image]
🚧

占领街头：封锁和阻断指南 - 街头实战指南 S05E15

[image]	关键词	团队 街头 街头战术 路障 非暴力
[image]	关联	[image]S05街头实战指南-总章节：武器装备、组织协调 … 全干货for激进社区晋升培训
[image]	创建时间	2025年1月18日
[image]	**Description**	行动安全性

封锁行动通过展现参与者甘愿以身试险的决心来赢得公众认同；这种行动承袭了非暴力公民抗命的悠久传统，相较于其他形式的激进派直接行动，更易被民众视为“威胁性较低”的抗争方式。

但需注意的是，随着镇压系统的残暴程度大幅加强，战术有效性和成本必需仔细衡量。

- Table of Contents

  为何、何地、如何
  锁箱封锁术
  材料
  操作指南
  侦察目标，策划行动
  收集材料
  设计、建造、改造与加固
  要点：
  实践和运送
  锁定后的行动
  警方反应与法律后果

其他封锁手段

[image]

这里是关于锁箱及其他街头封锁器具的组装与运用的指南。

抗议战术的谱系极为宽广，从举牌喊口号到刀光火影，多种多样，具体取决于战略目标。如果您希望强化施压效果、或在遭遇挑战时更有效地坚守阵地，不妨考虑以下方案。

请注意，本指南初版刊载于20年前出版的《灾难配方》。从2025年的视角回望，公民抗命已变得更为危险：极右翼政客不断立法限制，警察等法西斯势力则愈发漠视人命。因为公民抗命能成功的前提是假定对手无法对您造成永久伤害；而在当前的情况下，这一假定在很大程度上都是虚妄。某些时候，即便您已经做好了被捕的准备，保持行动的灵活性和风险容忍度也往往比束手就擒更能取得实质性的政治成效。

不论如何，本集内容目前在许多地区和情境下仍具有参考价值。

[image]

返回 - 自卫措施：[image]被捕支援

为何、何地、如何

实施封锁行动的动机多样，如：揭露或阻止不公事件、通过占领某个要塞空间或制造干扰以支持其他直接行动项目、减少交通死亡事故，等等。

可实施封锁的场所包括：高速公路、工厂和商场大门、商业区、即将举办企业晚宴或接待代表团的餐厅入口。勇敢的封锁者经常将自己锁在挖掘机等毁林设备上，或锁在政治行动占领建筑的入口处以阻止当局进入。

封锁最常用的工具之一是锁箱。

锁箱封锁术

实施封锁时，锁箱能发挥重要作用—— 请注意！前提是您面对的对手不会对您造成严重伤害，而且您已经为被捕做好了充分准备。

本集内容介绍的设计已在多个城市使用，包括警方“擅长”处理抗议活动的地区。即便如此，警方仍需耗费数小时才能将使用此装置的封锁者从繁忙街道移开。

这里介绍的是最简易的设计之一，实际存在多种可能性。可制作内含90度转角的锁箱，容纳单人双臂，使抗议者能舒适地将自己锁定在铁门、卡车车轴甚至铁轨上。针对重大行动，可制作内置锁箱的大型混凝土桶，或在地面开凿竖井，用混凝土和钢筋构筑单向锁定装置，亦可将报废车辆开至指定位置，使其无法移动后实施锁定。

锁定装置能阻断区域进出通道，形成吸引媒体关注的视觉焦点。其延缓交通的特性可为支援团队创造条件，使其得以举办提高意识的集会，向堵车司机分发传单或开展其他现场互动。当封锁者撤离后，警方通常会继续封锁该区域一小时以上，从而延长了行动的影响力。

封锁行动通过展现参与者甘愿以身试险的决心来赢得公众认同；这种行动承袭了“非暴力”公民抗命的悠久传统，相较于其他形式的激进派直接行动，更易被民众视为“威胁性较低”的抗争方式。

[image] 2018年6月，西雅图第二大道ICE办公室外爆发抗议。阻挠这些冷酷无情的雇佣兵拆散社区的行为，若世间尚存道义，此举便是其中之一。

材料

- 金属或塑料管材——如PVC管

- 螺栓和螺母——每个“锁箱”至少需要一个螺栓和一个螺母
- 铁链或绳索
- 登山扣
- 胶水 —— 可选，但建议使用
- 钢锯
- 电钻
- 断线钳——可选
- 至少一名愿意挺身而出的参与者

操作指南

锁箱是一种管道装置，可将人牢固锁定在其他同伴或固定的物体上。标准锁箱可容纳两人；通过多个锁箱与人员的协作，可形成人链。

锁箱利用人体躯干宽度与手臂跨度占据空间。锁定时需将自身固定在管道内的机械装置上；警察若想解锁，必须将手臂伸入管道，但管道几乎紧贴单个手臂的特性使其无法实现。如果警方试图强拽，金属锁链与螺栓将承受全部压力而非肩关节——前提是锁箱结构正确。如果使用登山扣连接管道内的螺栓，您就可以随时脱离锁箱。

通过锁箱，群体能迅速占领空间形成封锁，抵御警方的驱离行动。

侦察目标，策划行动

第一步是侦察您想要封锁的区域。

[image]

返回 - 自卫措施：[image]地形侦查

锁箱可应用于多种环境，但本指南假设您在城市环境中操作。

可封锁活动场所入口、商业区入口，或隧道、高速公路及匝道入口。首要任务是锁定最易形成交通瓶颈的节点 —— 无论是车辆、行人还是其他交通流。通常成功封锁一条主要街道即可引发大范围交通瘫痪。重点关注通往主干道的街道，并观察交通流向。如果计划封锁道路，需收听交通广播：识别易拥堵路段及通往主干道的支线。详细记录目标路段信息，包括：信号灯时长、特定时段开放车道、车辆主流转向方向。

选定最符合行动目标的地点后，需评估封锁所需的人力规模。如果选址得当但人手不足，车辆仍可通行，则该行动只会形成滋扰而非真正封锁；如果人链无法在两端与固定点形成“完整闭环”，即便连接参与者的锁箱牢固，仍可能轻易被驱散。

[image]

为快速测量距离又不引人注目，可采用脚跟对脚尖的步数计数法，或横向拉一根细绳/细线做标记。

同时需考虑锁扣装置尺寸及参与人数：若街道宽20英尺，锁扣装置长3英尺，那么通常需要五至六人配合。

精心规划队形。如果采用直线锁定，两端人员可锁定在固定物体上 —— 例如用自行车U型锁套住颈部，或采用链锁等安全性较低的方法。如果使用自行车锁或其他需钥匙的锁具，务必安排同伙迅速藏好钥匙，或预先将其藏于对手无法发现的隐蔽处。如需较松散的封锁，

可保持队形两端开放并采取坐卧姿势。亦可封闭两端形成环形锁定，或交叉排列成X形双列阵型。

规划时一定要考虑到长时间固定姿势的负荷。如果锁具没有足够支撑，被锁的人会因持续支撑而迅速疲惫。食物补给与血液循环问题同样需要周全考虑。

[image] 2025年4月2日，哥伦比亚大学一群犹太裔学生将自己用锁链捆绑在校园大门上，以示对巴勒斯坦学生的声援，要求校方公布向ICE举报马哈茂德·哈利勒的校董名单。在某些情况下锁链或许足够，但锁箱战术通常能提供更持久的防护。

收集材料

制定计划后，下一步便是收集材料。这些物品可能价格不菲，因此要多方寻找免费获取的渠道。建筑工地能找到PVC管；锁着的垃圾箱可拆下铁链；工具则可借用。若不想引起注意，不妨在多个地点分散购买物资。

[image]

返回：[image]匿名购买

购买螺栓、登山扣和胶水不会引起注意，但如果在柜台前搬运三十英尺长的PVC管，就难免引人侧目了。据传网络上出现大规模动员时，商店员工会很快接到警方监控此类采购的指令。购买喷漆、撬棍、断线钳或玻璃蚀刻剂时也需同样的谨慎。

如果不想留下交易记录，切勿使用银行卡、不要使用任何数字支付。

设计、建造、改造与加固

要点：

1. 将管道切割至合适长度。

1. 在管道中部（或根据使用者双臂跨度调整位置）钻穿管道两壁。

1. 将螺栓穿过双孔。

1. 锁紧螺栓。

1. 裁剪一条可环绕手腕并触及螺栓的链条。

1. 用登山扣将链条固定于螺栓。

1. 为共用锁箱的同伴重复步骤5和6。

1. 加固锁箱。

[image]

建造锁箱可以成为一项有趣的团体活动。

确保使用锁箱的队友进行试用，并根据手臂长度及其他变量进行调整。

[image]

手臂伸入锁箱的程度取决于个人偏好和战术策略，但管道平均长度应保持在4英尺左右。**PVC**管道覆盖手臂的范围越大，身体免受警方行动威胁的区域就越广。例如：如果二头肌暴露在外，警方可能通过施加疼痛控制手段迫使您解锁；而当整条手臂都置于管道内时，这种手段就无法实施。

每个人的手臂结构各不相同。进行锁定操作时，必须确保手臂能充分伸入管道以触及螺栓，从而轻松连接或拆卸登山扣。

如果使用者能在制作时到场就更好了，请测量其手臂尺寸来定制管道。如果无法到场，那么建议将箱体长度设计为通用尺寸——例如3至4英尺（约0.9-1.2米）。使用PVC管道时，可用普通钢锯轻松切割。如果需更持久的锁定装置，请选用更耐用的管道材料。

[image]

管径选择至关重要：手臂至少能舒适伸入至二头肌位置。除非手臂特别纤细或粗壮，管径应控制在4至6英寸之间。

切割管道至两人均能自由伸臂并指尖相触后，在指尖接触点固定螺栓。螺栓长度需超过管道直径；如果使用5英寸管道，螺栓长度至少需达5.5英寸。避免选用螺纹锋利或单端尖锐的螺栓。螺栓需选用粗壮且不易切割的材质，因其可能是整个装置中最薄弱的环节，务必确保其牢固性。

在管道单侧壁钻穿贯通孔。如需先钻顶部孔洞再翻转管道钻底部孔洞，务必确保两孔对齐！将螺栓穿过双孔。螺栓在管道中应略偏离中心，以便锁定者能用手指环绕并留出指关节空间。随后用螺母固定螺栓，螺母可置于管道内侧、外侧或两侧。可用强力胶增强螺栓牢固度；若条件允许，焊接固定效果更佳。

设计中可加入多个螺栓，增加警方拆除锁定点的难度。若采用多螺栓方案，还可尝试将手臂同时锁定在所有螺栓上。

接下来需制作连接管道内螺栓的锁链手镯。剪取一段链条，一端可环绕手腕，另一端环绕管道内螺栓固定，整体呈P形。反复调整链条长度直至舒适贴合。确保手腕扣环永久牢固，使用登山扣连接螺栓处的链条，以便紧急情况下能从锁箱中解开。

使用登山扣连接中央螺栓是极其稳固安全的方案，但也另有替代方案。如需更简易（但强度较弱）的变体，可省略中央螺栓，直接将链条穿过管道连接双方手腕。此方案适用于行动准备时间紧迫或资金有限的情况。中央螺栓的优势在于受力时能吸收部分冲击，抓握螺栓可提供控制力；如果两人直接通过锁链相连，任一方受拉扯时双方都将承受全部冲击。

装置组装完毕后，需确保钻孔位置、螺栓固定及锁链连接均舒适贴合。在手腕处的锁链位置加垫保护，必要时对管口进行软垫处理。至少应将锁链包裹在旧袜子中，并打磨管道边缘防止割伤手臂。

最后一步是强化您的装置。如今许多警察部门已掌握锁箱的构造原理，懂得如何拆解它们。这并不意味着锁定措施毫无效果 —— 毕竟警方仍需耗费时间响应、取用工具并逐个切割锁箱；但值得动脑筋思考如何领先于他们的技术手段。警方很可能尝试切割管道以暴露您的手和登山扣，或从螺栓处破坏箱体。请考虑延缓这一过程的方案：例如用钝化锯片的材料包裹锁箱，缠绕多层胶带和金属线，涂抹粘稠的焦油和沙子，或焊接钢筋护甲—— 甚至全部采用 …… 材料层数越多所需的切割方式就越多样化，防御效果就越好。

对于能固定位置的重型锁箱，可在管道外包裹混凝土层，再包一层塑料或铝制排水管。

[image] 一名警察正试图撬开一个锁箱。

实践和运送

所有箱体搭建完成后，请反复练习锁定与解锁的操作。每个参与者先单独练习直至熟练掌握，再与搭档协作，同时锁定箱体的两侧。

行动前需与所有参与人员共同演练速度与协调性，确保关键时刻万无一失！

为避免混乱，可在每个锁箱两端标注方向，规划人员朝向及锁合顺序。

一定要安排部分队友在锁定工作之外：他们不仅能协助快速集结，还能为无法活动手臂的成员提供食水补给，并协助应对警方及其他人员。

将所有锁箱运抵封锁点的过程可能颇具挑战，容易被拦截。如果可以

的话建议提前藏匿于附近，或伪装成木偶/横幅在游行中运送。如果有车辆可用，可在团队突然汇聚至选定地点的瞬间，用车将所有锁箱送达。如果需要维持长距离的封锁线并且手边有多辆汽车可用，那就抢速度：即让封锁者在开车到达该区域之前两人一组在车子内完成锁定，抵达后迅速下车，在数秒内就可以完成连接。

大批人群携带笨重锁箱行进时极易引起不当关注 —— 尤其是在当局正严防公民抗命行动的关口。但紧急情况下可设计巧妙伪装方案。

[image]

与所有封锁行动相同，若阻断正在使用的道路或高速公路，首要任务是拦截车流。

最简便的方式是协调另一组人员协同行动—— 要求小规模团队既要拦截车流又要保持锁定状态并阻挡车辆，就负担过重了。

要注意，此时愤怒的司机可能比警察更具危险性，一定要避免给他们制造鲁莽行为的机会。

锁定后的行动

支援人员可通过集会、街头派对或宣传活动来帮助增强封锁效果。

如果封锁街道，过往司机将成为街头剧的观众或传单接收者；如果封锁官方活动入口，记者可能记录你们发表声明的场景。无论哪种情况，总会有好奇的路人想要了解事件缘由，甚至在这个过程中获得些许娱乐。

[image]

如果封锁行动可能引发交通拥堵，且担心行动被误解为针对普通司机的攻击，可考虑分发某种形式的和平礼物，一小瓶饮料基本就能解决问题，切勿冲突。

参与行动的人可身着象征性的服饰或悬挂标语横幅阐明行动缘由。如果人链两端没有与固定物体连接起来，理论上可保持锁链状态移动，但实际上操作难度有点大，且存在安全隐患。如果您有移动计划，务必提前演练，并指定协调员指导动作或指挥行进节奏。

无论是否预见到此类需求，只要参与锁链行动的人数超过两人，提前建立基础的沟通与决策机制都是明智之举。

[image]

警方反应与法律后果

最终，警方的反应无法确切预测，因此在团队中耗费数小时争论此事恐怕没什么意义。

关键是要安排一名警务联络员与当局交涉，或至少确保对方理解现场的情况；同时需要记者或其他目击者在场，以缓和警方行为或至少记录其举动。如果警方采取危险行动，请冷静告知他们：您的手臂被困在管道内无法抽离，且一支精锐律师团队正摩拳擦掌准备将他们告上法庭。警方总会试图恐吓您 —— 保持镇定，揭穿他们的虚张声势。他们可能使用胡椒喷雾等武器，但此举将招致公众强烈谴责，尤其当您勇敢承受迫害时。

如果锁链两端均有固定点，警方可能先解除固定点人员。如果能将整条锁链移开且解除你们阻碍交通的状态，他们很可能会这样做——但如果你们采取坐姿或仰卧姿势他们就很难实现了。如果无法把人链整体移除，他们就会尝试逐个锁扣切割，将整个人链分割为更易移动的短链。警方拆解人链的方式取决于其经验水平。任何警局都不愿惹上官司，因此他们通常会尽量避免造成伤害。如果您能隐藏中央螺栓的位置，他们便无法确定您的手在管道内的具体位置，这将阻止他们直接将管道锯断。

通常警方会呼叫消防部门，使用专门用于从废墟中救人的特殊工具。

> 上次我参加锁定抗议时，警方用特制的木架支撑住我们的PVC锁箱，再用钢丝钳、锯子等工具逐步拆解人链。

封锁行动结束参与者被捕时，所面临的指控也难以预料。至少过去常见的指控是“妨碍公共秩序”——这与用身体阻塞街道等通道的罪名相同。使用锁箱本身并非独立罪行，但警方可能进行威胁或附加“持有犯罪工具”等额外指控。

> 在我参与的两次锁定行动中，警方均声称使用锁具将追加“持有犯罪工具”指控，但正如警方惯常所为——这纯属谎言。无论如何解读，PVC管、铁链和登山扣都不构成所谓的犯罪工具。

2024年亚特兰大“阻止警察城”运动中，多名实施锁定行动的示威者屡次被控轻罪‘非法侵入’，但当两名活动人士攀爬布拉菲尔德&戈里建筑工地起重机并锁定自身时，检方却以重罪——“非法监禁”罪名起诉他们。荒谬的是，警方竟宣称全程在地面操作的起重机司机因两名悬挂在250英尺高空的活动人士而“无法离开”。

无论如何，您都应该组建一支随时待命的法律支援团队。

[image] 路障与封锁在美国劳工斗争中有着悠久的历史。这幅插图描绘了1886年3月4日纽约市罢工的有轨电车员工与警察对峙的场景。

实施封锁是一件严肃的事情。您必须做好心理准备：在无法自由行动的状态下，长时间承受与愤怒警察周旋的煎熬，随后还将面临被捕入狱的更严酷考验。请怀着内心的平静和决心开启封锁行动，确保饮食充足、水分补给到位，做好应对危险风暴和戏剧性事件的准备 ——若预料行动将持续较长时间，请务必穿上成人纸尿裤！

其他封锁手段

封锁行动存在多种实施方式。最传统的是搭建路障。如果个人希望将自己锁定在某物或某人身上，可将自行车U型锁套在颈部，但此举同

样需要传统锁定行动的配套支持体系。

在土路上挖掘沟渠可形成路障；还可在沟渠中埋设栅栏、金属或木杆、支撑杆缆线等障碍物。

如果警方陷入足够焦虑或混乱，他们反而可能亲手帮您封锁特定区域。

[image] 法国拉扎德抗争区（la ZAD）的一处路障。

封锁繁忙道路时，首要任务是将车流减速至安全速度。自行车队可减速至停顿状态，其自身即构成路障，为后续建立永久性封锁创造条件。旧自行车可加装金属配件，骑行结束后锁在一起作为路障。

在繁忙公路上悬挂横幅能显著减缓车流，甚至引发堵塞——车辆堆积本身就是某种路障，毕竟再没有比更多汽车更能阻碍汽车的东西了。

说到车辆，可将旧车开至指定位置使其报废；若能用现金从肯定不会向当局提供有用线索的人手中购得车辆就更好了。这些车可预先装载路障材料，停放后即可就地部署；参与者甚至可锁定在车上。

待车流减缓或停滞后，可在公路上架设钢缆或围栏，将其固定于电线杆、路灯柱或护栏上。

别忘了快干混凝土能有效封堵门道等通道。掺入螺栓螺母等材料可增强耐久性。

若在低风险环境中追求趣味效果，可将办公室或商铺大门用砖封堵。深夜施工，确保砂浆充分凝固。

封锁街道或桥梁两端时务必预留出口。阻断车流的同时不可困住平民—— 以及您自己。切记避免封堵通往医院等重要设施的通道。

[image] 厄瓜多尔的路障。让一群防暴警察搬不动。

[image]
[image]

如何启动黑群 - 从准备到行动：街头实战指南 S05E16

[image] 关键词	匿名着装 协调 直接行动 组织 街头 街头战术
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月19日
[image] **Description**	行动安全性

关于如何 [image]匿名着装 的详细指南。

- Table of Contents

全部必需只有三部分：
可选材料：
行动
“群”是什么？除了“黑群”，还有其他类型吗？
“群”集体行动的作用是什么？
黑群战术可以在哪里使用以及如何应用？
我们可以从这种先前的成功和失败中吸取一些教训：
结构
准备工作
行动期间
撤离
事后

[image]

全部必需只有三部分：

1. 可掩盖穿戴者身份的恰当的衣服；

1. 信任和沟通；

1. 一项任务—— 战略目标。

可选材料：

物资：水（多带一点水，特别是当您穿上防护装备时、或预计会受到化学武器攻击时，水很重要），食物（不要依赖商店），等等。

伪装：为不同目的或不同阶段的行动准备不同的衣服；把这些衣服套着穿，以便脱掉外面的一层后就可以迅速进入下一阶段或不同行动。

防御性装备：旗帜、盾牌（旗帜可以塞进毛绒玩具的身体里、盾牌可以伪装成标语牌）、安全靴（应该足够舒适，适合跑步）、防弹衣或衬垫、防毒面具或护目镜和浸泡了酸橙汁或醋的头巾 —— 储存在密封袋中，直到必要时再戴上）、雨衣或化学防护装备（如果有化学袭击的风险的话）、任何您知道如何应用的相关医疗用品等。

进攻性装备：喷漆、投射物、弹弓、装在粗杆上的标志或旗帜（或只是普通的杆子）、燃烧瓶、强光灯（在夜间行动中遮蔽警察视线或摄像机的视线）、梯子和/或用于攀爬或突破障碍的断线钳等。

通讯设备：对讲机、一次性手机、警察扫描器（用于扫描警察使用的无线电频率的装置）、旗帜、鼓、用于发布内部通知的共享代码(暗语)。

交通工具：自行车、足够的现金零钱（坐地铁）。

[image]

返回 - 关于穿衣的原则：[image]在街上保持安全：街头实战指南 S05E12

[image]

行动

“群”是什么？除了“黑群”，还有其他类型吗？

您可能听说过黑群，这是一个古老的、甚至可以说是老旧的无政府主义传统，在这个传统中大量的直接行动爱好者聚集在一起，所有人都穿着黑色衣服，戴着面具/面罩，从事某种程度的对抗性活动。

在过去的几十年里，这种战术赢得了一些著名的胜利，失败的次数也多得让人数不清。今天，与黑群战术相关的具体文化特征可能使人们很容易忽视黑群战术的悠久历史和它的广泛用途。

例如，波士顿茶党（1773年）就是一个集体行动的例子：参与者秘密组织起来，穿上相应的伪装（尽管他们选择把自己装扮成“印第安人”不那么政治正确），并从事大规模的挑衅性财产破坏活动；据推测，他们的沟通和互助防御策略与几百年后在西雅图进攻同样有害的咖啡公司的著名黑群团体所使用的策略没有什么不同。

[image]

“群”集体行动的作用是什么？

当行动的参与者预计警察、法西斯分子或其他对手会努力想要识别参与者的真实身份时 —— 也就是说，如今这个高科技监视时代的几乎所有情况下 —— “群”就是针对这点实施的保护。当一个团体中的每个人看起来都一样时，就很难将特定的人挑出来。

许多激进活动最好以不太引人注意的方式进行，但在有些情况下，有必要在公开场合吸引目光。“群”战术最适合于所要求的行动处于公开和隐蔽之间的灰色地带的那种情况，因此必须谨慎应用：如果您以“群”形式和队友一起参与完全合法的行动，完全融入其中是最好的—— 其中每个人都难以成为特别的目标；另方面，如果您确认整个行动相当激进、很有可能会被识别和被抓捕，也许最好在传统的“群”形式之外进行，在一个完全封闭的团体中，设置出人意料的元素等——发挥想象力。

公开的“群”活动的一个积极方面是，与完全地下的活动不同，它可以创造开放式的局面，在这种情况下，少数人的行动可以为其他人的加入打开闸门。它可以是一种参与性的和具有感染力的体验。

最明显的方法是组织一个公开的或半公开的“群”。在公开的情况下，向所有感兴趣的人发出号召，让人们聚集在一起，在“群”中采取行动；举行公开的会议，讨论目标、战略等。这种方法的好处是可以让更多的人参与进来；同时，明显的缺点是安全受到严重影响，行动的可能性受到严重限制。

在半公开的“群”中，组织工作在相互认识和信任的人之间秘密进行，但当“群”形成并聚集在一起时，欢迎其他穿着本“群”服装的人参入进来；在过去几年的黑群活动中，这是最常见的形式。

请注意，在这样的“群”中，参与者仍有必要做好应对渗透的准备，但他们至少有安全规则的规划和核心层结构的好处。在一个完全封闭的“群”中，所有参与者的一切准备工作都是秘密的，在行动中不欢迎任何外人的参与或跟随。即使需要这样的“群”，作为一个公开行动，而不是秘密行动，仍然是有价值的：行动的公开性可能会发出一个重要的信息，“群”外的其他人可能会受到启发，组建他们自己的类似行动。人越多越安全，人群掩护本身就更容易帮助那些选择秘密行动的人隐藏起来。

[image]

返回 - 镇压手段：渗透者

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

返回 - 自卫措施：[image]信息最小化原则

在一个“群”中行动的好处有很多。最基本的，群体参与可以令人振奋，对道德有好处—— 在一群表面上准备做他们认为正确的事而不顾警察恐吓的人中行动，往往要比跟着一群乞求者无力地呼喊更有力量，同时搭配战斗服是一种激发勇气的仪式 —— 我们中没有人会被抛弃。

一个“群”的存在可以传达重要的信息：对当权者来说就是，“不要试图操弄这个游行了，这是一个相当有凝聚力的行动”；对盟友或可能的盟友来说就是，“不要绝望，我们和你在一起”。

最后，也是最重要的就是，匿名：在大规模行动中，有无数的理由要隐藏您自己的身份。即使您的一切行为完全合法，即使您并不介意被警察拍下照片进入镇压黑名单存档，您仍然很有必要通过掩饰和增加被掩饰的人的数量，为其他人做出很大的贡献—— 使警察更难跟上你们所有人的步伐。

判断具体情况很重要。有时蒙面的人群对公众来说是不必要的恐吓；有时蒙面的人太少，或者警察的注意力集中在“群”形式上，您可能会认为足够低调更安全；而有时，最好让邻居看到您的立场，或者让公众和摄像机看到并非所有参与激进活动的人都是年轻男性。否则，如果别人都戴上了面罩，您也不妨这样做。

这些面罩不一定必需是黑色的滑雪面罩，有很多更有趣的方式可用来掩盖您的身份。除了黑色面罩，还有无限的可能性：粉色面罩、小丑面罩、医用隔离面罩、维修工面罩 …… 只要有一群人穿着相同的衣服/装束，就可以利用这样的人群进行伪装，采取面罩战术。例如，万圣节可以提供一个很好的机会以采取 Bloc 行动，必需穿校服的校园庆典中也是如此。

[image]

黑群战术可以在哪里使用以及如何应用？

在过去的几十年里，黑群行动在群众行动中大受欢迎：在世贸组织等集团的会议上，在总统候选人之间的辩论等政治活动中，在反战示威和声援遭受警察暴力的社区的游行中，都有黑群形式的抗议。只要有大规模的抗议者聚集，部署或号召一个“群”就很可能更有意义。

在这样的环境中，“群”可以达到很多目的。如前所述，它可以只是作为团结的承诺或声势出现；可以作为其他活动家的防线，或分散镇压者的注意力；它可以进行破坏性行动—— 这可以达到经济目的，例如给邪恶的公司造成经济损失，或其他实际目标—— 例如让地方当局知道举行某类活动是有社会成本的；或者让被疏远的工人（包括活动家）可以亲身体验到，被压迫者束缚的现实是可以被打破的。

一个“群”可以提供以直接行动而不是单纯的语言来争夺权力和控制权的可能性，从而保持精神饱满；它可能会试图引发全面的起义，或者简单地创造一个奇观，以强调无政府主义的存在并突出其浪漫的吸引力—— 尽管自由主义者抱怨 “疏远公众”，但西雅图的黑群和之后的行动在提高无政府主义行动的群众吸引力方面所做出的贡献不亚于任何宣传出版物。每一个黑群行动都可能成为未来此类行动的良好实践，有希望取得更大的成就。

“群”在选择大规模行动的目标时，关键是要考虑到当地人和其他将参与或在场的人的意图、需求和舒适程度。

如果毫无必要地疏远人们，不仅会产生反效果，而且会危及“群”参与者；

如果您的行动无法尽可能获得当地民众的支持，您的“对手”就不只有警察了（警察已经够多了，别给自己增加不必要的对手）。

您最不应该做的事就是用您的行动危害他人—— 不要躲在人群的后面向警察扔石头，不要冒险挑起警察对和平游行的攻击，特别是如果您没打算坚持下去承受攻击的话。

如果您在一个主要是外地人的团体中活动，在一个居民区中行动，不要自大到认为应该由您来决定什么程度的冲突最适合 —— 最好表明您尊重当地人的需要和观点，并愿意听从他们的领导。也许在某些情况下，理论上为某项行动带来某种程度的强度是合适的，而其他人并不这么认为—— 例如，如果改良派的组织者试图用无用的姿态去 “解决” 严重的不公正问题，这对改变毫无帮助，于是您有自己的方案 —— 但是，要首先确保为任何事情付出代价的人是您和您的同伴，而不是无辜的旁观者。

[image]

同样，考虑到您的经验、队友人数和其他资源，对您希望在手头的情况下完成的任务要持现实态度。如果当地民众憎恨在他们城市开会的领导人的傲慢，但同时并不信任聚集在那里举行抗议的“外地人”，那么在当地人可能认为是“外来者” 对他们家乡街道的攻击中，针对那些领导人的行动可能比打碎公司窗户更有意义。

[image]

把一切都考虑进去，至少包括：

警察部队的行为特征是什么，当前当地的政治气候是什么，

其他人对发生在您和您的同伴身上的事的了解程度如何，

当局这次有可能是想给您一个教训，还是想要压制消息避免媒体报道，

警察是想保护整个地区（在这种情况下，如果他们有足够的人数，大规模逮捕很可能会发生）、还是仅仅想要保护其中的一部分（在这种情况下，如果警察人数不足或不确定，他们可能会采取分散的或防御性的战术）。

您的行动是为了吸引媒体报道吗，还是为了向现场那些亲眼目睹的人传递信息，

或者为了那些参与行动的人，还是为了那些买单的人？

您的目标是否值得冒险，是否适合有关的事件？

如果是在大规模的群众之外，以“群”的形式行动是一个更危险的提议，因为“群”非常醒目，很容易被警察包围和消灭。从历史上看，在示威活动中，几乎每一个与更多的守法抗议者混在一起的“群”都能保持一定程度的安全和一致性，而几乎每一个试图在守法抗议者不在场的情况下单独行动的“群”都会遭受或至少面临严重的警察镇压风险。

[image]

我们可以从这种先前的成功和失败中吸取一些教训：

1、如果没有出其不意的战术、和广泛的人群掩护，就不应该使用黑群形式。

至少要有足够大的人数、高涨的士气和丰富的防卫经验，您的行动目的肯定不能让很多参与者被捕。

2、在群体活动中宣布的直接行动（黑群、未经许可的游行等）应该总是在大型的一般抗议日或之前进行，而不是在其之后。

当直接行动在大规模的游行和集会之前或同时进行时，它往往为接下来的一切定下了基调，提高了活动的档次，并使整个活动变得激进；相反，当直接行动参与者是在守法的活动家撤离后唯一留在街上的人时，警察就会知道他们可以孤立、虐待和逮捕直接行动参与者。

有众多其他目睹警察暴行的人的存在是一种重要的威慑力；如果没有这种威慑力，您将面临危险。

3、那些在黑群内活动的人需要得到团体之外的一些人（如果不是大多数的话）的支持或至少是尊重，这样才能保证他们在场上的安全，更不用说在活动家社区的普遍良好意愿了。

在一个历史性的例子中，一个黑群被警察包围并逼到墙角，警察正准备冲过去攻击这些人，这时一个自由派妇女组织的游行被改变了路线，从该地区通过，为黑群成员提供了混入和逃跑的机会。

[image]

因此，如果黑群行动的目标或对象能让外人立即理解，就会有很大的帮助，所以不管其他人是否同意这种战术本身，他们至少可以理解为什么要采用这种战术。

[image]

另一方面，在有些情况下，这些经验法可能都不适用。在大规模行动的领域之外，只要有意外因素存在，还有许多其他环境可以应用黑群战术；事实上，这种应用可能是对黑群的未来最有希望的，因为现在警察已经非常熟悉并准备好让黑群行动出现在示威活动中了。迅速行动并对毫无戒心的目标进行突击的黑群行动者可以完成大量任务，特别是如果它有适当的规模时。

当您在一个没有其他大量示威群众作掩护的黑群中行动时，您最重要的优势是出其不意。如果您的组织方式让有关当局看不到您的意图，您就有可能在他们能够作出反应之前完成所有工作并逃跑。即使镇压者真的扑过来了，他们也有可能没有准备好进行大规模的逮捕，所以您可以期待他们只试图抓捕个人。在这种情况下，进行高风险行动的个人可能会趁势逃跑（公民抗命的热心人甚至可以在小规模的逮捕中对警察进行阻挠，不过如果他们与黑群有联系的话，可能会有面临阴谋罪的风险）—— 或者，如果一个团体能够以高度的团结和大胆的行动紧紧靠在一起，不允许警察抓到其中的个人，就有可能协商好集体撤离，不过您至少应该预期到你们会被跟踪。以前曾发生过这样的情况：一群活动家一起违法，表明他们不会被恐吓，也不允许其成员被逮捕，毫无准备的警察允许他们离开一个地区，作为结束行动的回报。不过，也发生过他们被橡皮子弹射中的情况。如果你们中的一些人正在计划进行非常激进的活动，那么就建议让你们小组中的其他人采用各种对抗性较低的战术，这样警察就不可能把你们都当成铁杆罪犯。

[image]

一定要确保你们小组中的每个人，特别是那些不热衷于承担巨大法律风险的人，事先清楚地知道可能的最高级别的非法活动是什么，因为您永远不知道警察是否会选择活动家团体中最和平的抗议者去逮捕，只因为 警察抓不住那些最激进的活动家 。

如果您在日出时分出现在一个公司的办公室里，您知道那里肯定基本上没什么人，您必须依靠速度和聪明的逃跑路线才能成功撤离；但在其他情况下，就像在示威活动中一样，会有人群掩护—— 甚至是潜在的支持性人群掩护—— 来帮助您逃脱。

在为某一特定背景下的黑群行动制定计划和目标时，回顾历史以寻找先例总是很重要的。如果曾经有人尝试过类似的行动计划后引发过一场灾难，那您最好再想一想，您可以加入什么新的元素，给自己一个更好的机会。历史往往会重演—— 除非您能用聪明才智的创造力来打破这一惯性。

您需要熟悉过去几年来黑群行动的历史；每当您考虑加入一个行动时，建议先参考以前的同类行动案例，那些曾经的故事最能说明您能从这个行动中得到什么，当然，要记住，您的对手也一直在做同样的事，所以，指望一个特定的战术能赢两次绝对是非常冒险的提议。知道什么时候不采取黑群行动和知道什么时候尝试黑群行动，同样重要：当没有足够的参与者或条件不利时，在黑群行动中不成功的尝试很可能只会消耗能量，不如把力量用在其他地方。当您采取黑群行动时，就要全力以赴，要给人们留下深刻印象，然后等待下一次恰当的机会出现时再次这样做。

[image]

结构

自然，亲密团队是任何黑群行动的基本组成部分。作为一个能够主动防御和自主决策的小团体的一部分，参与黑群活动的重要性再怎么强调都不为过。由自给自足的亲密团队组成的黑群可以迅速做出民主决策，可以分散成同样有效的更小的团体，可以处理紧张的情况。

[image]

不言而喻，在您的亲密团队中，您应该建立共同的期望，即：目标是什么，什么程度的风险可以接受，什么样的安全是合适的。

在黑群活动中，安全问题尤其重要，因为这是一个灰色地带，可能涉及到公共活动和非法活动的粗略混合；一定要确保每个人 都有相同的安全文化意识 。

无论黑群的总体规模如何，每个亲密团队都应该完全自立，至少在一个团队打算实现的目标方面。

逃生路线、法律资源、紧急备用计划、对该地区的了解（地形侦查）——每个亲密团队都应该拥有所有这些。

团体内部的伙伴系统是很有用的，如果团体本身是分散的，个人可以对其伙伴的安全和下落负责。

可以分配内部角色。例如，侦察员负责跟踪活动和警察的存在（他们可以配备对讲机或手机，以便与主要团队联系，并可以骑自行车以提高速度和流动性。通常最合理的做法是将亲密团队成员安排在距离大部队一个街区左右的地方，这样他们就可以提供危险预警和对该地区更广泛的观察），通信人员（也配有对讲机或手机，也许还有一个警察扫描仪）与侦察员和其他团队交换信息，专门的通信员跑步向附近的团队传达新信息。

有经验的成员负责分析信息，并负责快速做出决策；有人负责按计划实际执行行动，有人负责望风，也许还可以有一个旗手或行军乐队来维持士气，并保持行动团体在远处的可见度，等等。

也许明智的做法是让一个穿着普通服装的人参加黑群行动，负责处理诸如向观众解释为什么他们不应该拍照这类任务，因为警察可以没收围观者的相机并在法庭上使用这些照片。亲密团队在大团体中扮演的角色也可以是专门的：亲密团队可以作为一个大型黑群的侦察员，或者负责着手封锁某个特定的十字路口，再或者集中力量在大团体的前

面打头阵。

一个亲密团队可以单独形成一个小型的、临时性的黑群，但是一个更大型的、更强大的黑群可以是一系列亲密团队的集群。在这种情况下，在集群内建立高效的和民主的结构是至关重要的。

即使在最紧张的情况下，也应该能够在亲密团队内部的个人之间和不同亲密团队彼此之间迅速沟通新消息、问题和答案。有些人主张采用更加军事化的黑群模式，这种模式的运作可能更像您的敌人对您施加的等级制度，但黑群的优势在于其分散化的、不可预测的性质；您不该期待在压迫者设置的游戏中击败压迫者，那很蠢，相反，充分利用您自己的优势，反制您的对手，才更容易取胜。

[image]

您最好可以改善您的队友之间的协调，而不是控制：行动者是为即兴创作搭建舞台的指挥家，而不是有下属和指挥官的军事战术家。

在一个由不同地区的亲密团队组成的黑群中，可以肯定来自本地的团体更多拥有预判事态的优势，并因此可能做了最多的思考和准备。这不一定是个问题，只要其他人信任他们，并且自己有足够的组织能力来保持其自主性。本地团体应该在安全的情况下，尽可能多地与其他人分享相关信息，同时也要确保不要让自己承担起对其他团体的权威地位；一个地方团体试图带领不知情的群众执行一个不公开的秘密任务，这可能是一个真正的灾难隐患。

[image]

准备工作

[image]

行动前最重要的事情之一是了解该地区—— 通过侦查 [image] 地形侦查 。

每组尽可能多的成员应花时间穿越该地区，仔细记下逃生路线和死

角、摄像头位置、警察可能聚集或试图保护的地方、可能的目标、可能的资源（如可移动的栅栏等路障材料），最重要的是确保不会迷路。

那些不能提前到场参加侦查的人至少应该记住地图。可以从互联网上获取航拍地图，用于无法获得街道地图或无法满足需要的地点。

确保在行动前有安全的住所，您完全可以确认这点，警察肯定会不惜余力地抢在行动开始之前连锅端活动家团队。太多次了，警察在行动前突击检查活动家的住房，并逮捕了数百人，尽管这些人还没做任何事。这在很多国家都是如此。所以，尽你所能找到一个可以不被警察注意到的地方睡觉和做准备，这样你就不会有这种风险。住在你叔叔的朋友家，或者在基督教青年会租一个睡觉的地方。如果您是外地人，同样要确保您的合作团队（可能与您的亲密团队不一样）已经计划好了安全地重新集结和离开该地区，并在紧急情况下有一个 **Plan B**。请记住，如果事情真的发生了，城市的某些部分可能在行动后对你们关闭，所以你们需要在其他地方重新集结。

[image]

行动前的预备会议是大多数黑群准备工作的一个重要部分。同样，这些会议的安全性和公开性取决于您希望有多少人参与（以及具有何种程度的直接行动经验），以及您愿意承担何种程度的法律风险。

[image]

返回相关自卫措施：[image]户外无设备对话 ；[image]信息最小化原则 ；[image]数字技术限制和最佳实践 ；[image]反监视

如果您想组织一个大规模但主要是象征性的公开行动，您可能会选择公开召集并通知会议时间；如果您要组织一个在街上公开但需要私下准备的黑群的行动核心，那就告诉您信任的人，让他们只向他们信任的人传递会议的邀请。如果您正在准备一个完全封闭的黑群行动，您不仅应该只向您的行动伙伴透露会议的时间和地点，而且还应该确保他们都知道不要向任何人提及这个计划本身的存在，并准备好不在场证明，这样他们的其他朋友就不会怀疑他们在做什么。

会议地点是安全方面的一个重要因素。您肯定不想要一个可能被窥探的地方（不要在私人住宅，尤其是敏感人士的住所），您也不会想要一个可以被一览无余的地方（不能是第二天行动地点对面的公园），您不会想要一个可以看到您进出的地方，或者有人可以意外进入的地方—— 派侦察员，一旦有危险苗头出现就锁门，注意任何可疑的东西。小团体可以散步聊天；大团体可以在安静的户外环境中会面——如果有时间的话，可以去徒步旅行或露营，也可以在公共建筑的包间里会面，比如图书馆的自习室或空教室。最好的情况是：你和经营咖啡馆的老板关系很好，虽然他不知道你参与了直接行动，但他不介意让你在某个下午时分在小店后面的房间里举行私人聚会，没有任何问题。

当聚在一起的时候，如果出席会议的所有人并没有彼此相熟，您可以通过执行 “担保” 制度来建立安全级别：让每个人把一只手放在他们认识的和信任的其他人身上。希望房间里的每个人都能通过这样或那样的关系被接触到，会议可以在某种程度的信心中开始。

[image]

返回：[image]“我的”朋友还是“我们”的朋友？：如何执行担保措施

如果您是参加更大的黑群行动的亲密团队的一员，您可能会想先举行自己的会议，所以当您的团体代表参加更大的会议时，她就可以根据您对更多人的信任程度，介绍您所拥有的信息、您所提供的资源、您希望实现的目标和您提出的计划。

如果这是一次大规模的行动，并且有一个更大的代表会议正在举行，那么至少应该有一个来自黑群或与黑群沟通的人参加；出于安全考虑，不论这个人是否表明自己的身份，至少她应该在那里注意到其他事情的发生。一个黑群的代表可以作为一个亲密团队的一员参加小组代表会议，希望为参与黑群活动的人提供支持，从而试探性地了解情况，甚至认识其他对黑群感兴趣的人。

在与您的亲密团队和黑群的会议上，您要为这一天制定某种计划（不必要求完全如愿以偿，但这些计划有助于让每个人在实践中思考问题），建立一个结构，以促进团体的沟通并迅速做出民主决定，如上所述。无论您的计划是否实现，结构将使您具有适应性，从而有效。

您应该为黑群行动建立一个集合点，制定疏散的计划，以及一个可能的时间和地点来重新组合，如果行动团体提前分散的话，这样做是可取的。分享法律信息，为被逮捕的人提供哪些资源。仔细研究每一种可能的情况，以及在每一种情况下您能从对方那里得到什么。

[image]

心理学在这里很重要：为最坏的情况做打算，但不要让自己士气低落 —— 您将可能出现的问题考虑周全是为了做好准备，以争取最好的结果。

[image]

行动期间

在行动前不久，用永久性记号笔将法律联系人的电话号码写在身上通常是明智的，这样您就可以确保在被逮捕时，无论发生什么其他情况，您都能有这个电话号码。

您也可能需要知道当天行动中的其他合作者的手机号码等：试着把它们背下来，或者，如果不行，就写在皮肤上，如果有必要，可以擦掉它们。

您还可能希望身上有足够的现金来支付食物、交通和电话费用，但不要太多，因为一旦被捕，这些钱可能会被没收。

如果您的身上有穿孔，把饰品拿下来，以免出现暴力镇压时造成伤害。

不要携带您的地址簿，也不要携带不必要的无政府主义宣传品，或任何不必要的有可能将您治罪的东西；如果您想在被捕时以“真实”身份被处理，请带着您的身份证，如果您打算在这种情况下向警察隐瞒身份，请确保您身上没有任何身份证明文件。

携带足够量的水和高能量的食物；为紧急情况做好准备 —— 如果您

与所有人失散，不得不在垃圾箱里过夜，您不会希望自己挨饿的，但不要用任何不必要的东西造成负担。

随身携带任何您知道如何使用的可能有用的急救用品。要了解街上会有哪些医疗援助—— 比如街头医护人员和诊所，如果您必须去医院，要有一个计划（如果您担心在医院会遇到警察，要准备假名字和假身份，以及不在场证明）；同样要了解街上是否会有法律观察员和媒体，以及您是否希望他们在您身边或远离您。

[image]

返回：[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06

要 为眼前的情况做好准备 。如果警察的人数超过你们的队伍，正在那等着你们呢，而且该地区有记者和平民，不要戴着防毒面具穿着防弹衣来—— 警察可能不会用毒气攻击你和殴打你，他们会试图包围和逮捕你，而你需要能够快速移动并很好地融合到大量人群中以避免这种情况。

衣服是黑群战术的一个基本特征，也是黑群赖以生存或成立的基石。您可以在远离行动的地方先练习一下穿着这样的衣服跑跳的自如度，这样您就不会在现场时感觉不适应。黑群的整个想法是让我们彼此看起来没有区别，所以要确保无论您的行动主题是什么，每个人都要对此有基本共识，而且您自己的衣服不应该因带有任何特征而被区分出来。在最坏的情况下，您可以把T恤衫做成一个面罩：眼睛从领口上露出来，把袖子绑在脑后。

您的衣服应该保护您免受您预期的危险，同时又不会给您带来不必要的负担；如果出现意外情况，衣服应该具有适应性。

分层穿衣是关键：如果可能的话，在全黑的衣服外面穿一层普通的外衣去参加黑群行动，然后在全黑的衣服下面再穿一层撤离时能帮助您瞬间融入普通人群的日常衣服 —— 当然，注意不能有高热的危险，那会影响您的行动力。最明智的做法可能是将撤离时的衣服装在一个密封的袋子里，以防在您需要使用它时，比如您身上沾满了油漆、催

泪瓦斯等（镇压者会发射漆弹以标记抗议者，那种难以清洗的油漆将在未来用于识别您）。

如果您预计会受到化学武器的攻击，请穿上防水的外层衣服，并在其下层穿上不会吸收化学品的合成纤维（棉质衣服会吸收化学品）。对于严重的对抗状况，选择带有防碎镜片和可更换的非石棉过滤器的防毒面具，它不会太遮挡您的视线；否则，您可以通过把头巾浸泡在醋或酸橙汁中来保护呼吸（将泡好的头巾装在密封袋中带到行动现场；您可以随身携带一两个酸橙以保持头巾持续有效），并佩戴泳镜（对于戴眼镜的人可以获得带度数的泳镜；不需要一直戴着，当不需要佩戴时，将其拉到前额上，以免其起雾）。

您可以在头巾下面加一个防尘口罩以提供额外的保护。理论上耳塞可以在应付闪光榴弹时提供一些保护，但无法说清一个人应该如何知道什么时候戴上耳塞、什么时候拿出耳塞，以保持适当的注意力。如果您预计有可能受到打击或警方正在准备发射榴弹，请穿上某种防弹装备（运动装备就够了）和泡沫或衬垫，并戴上自行车或摩托车头盔。

[image]

上述具体分析详解：[image]头部是人最大的弱点 — 了解头盔和使用技巧：街头实战指南 S05E02

以及：[image]抵制催泪瓦斯和橡皮子弹：街头实战指南 S05E03

[image]

准备在与警察的冲突中保卫领土的黑群行动可以使用盾牌。这些盾牌可以用垃圾桶盖或切开的交通锤、充气筏或内胎制成，用防水胶带和可能的一层篷布、结实的老式纸板、或分层（超级胶粘在一起）和加固的有机玻璃进行固定。

在手柄上缠上厚厚的胶带，这样冲击力就不会伤害您的手腕，手柄上要提供足够的空间，这样您的指关节就不会承受所有的冲击力。较大的盾牌更适合于防护投射性武器或作为移动路障，而较小的盾牌则具有更好的机动性，在徒手战斗中发挥更大作用。

一行人手持盾牌可以组成一个盾牌墙，特别是当所有参与者练就了共同行动的能力时，协调性最好；另外，也可以建造大规模的多人盾牌，如下面将要提到的绝缘板标语牌。这样的盾牌应该有足够的接头，以便在较窄的街道上前行；请记住，这些接头也是这类盾牌最薄弱的地方。

[image]

返回 - 盾牌/盾墙制作方法：[image]加固横幅和盾牌的制作和使用方法：示威参与者指南S05E14

[image]

虽然可能有点滑稽、但经常发生的情况是，在一起讨论和准备行动的队友们在行动当天当所有人都穿上黑群装备时就 认不出彼此 了。 你们不妨在早期就互相表明身份，特别是来自不同城市的合作者和亲密团队成员、准备好一起行动的人，这样在混乱中更容易跟上对方的步伐。

黑群形成的时刻可能是最关键的部分。在哪里和什么时候戴上面具是个难题：如果您戴得太晚，一旦加入黑群团体，您就有可能被识别；如果您戴得太早，在加入黑群之前，您就有可能被警察抓住。在活动前后四处走动的小型蒙面团体是警察攻击的最佳目标。

[image]

在大型示威活动中，最好的选择之一是在还没有受到太多监视的大群人中穿好装备，周围有您信任的人，然后在人群中移动，与您的团队伙伴们会合。

穿衣的层次在这里也很重要：如果您能在最外层穿上普通的衣服，使您看起来像个平民，戴上面具就意味着丢掉那层衣服，同时迅速戴好面具。

在一个您可以出其不意的行动中，您总是可以在你们团队的汇合点附近挑选一个安全的、安静的地方，在那里戴上面具。

在大规模行动的情况下，在其他抗议者上街之前，黑群的汇合不应该发生；再一次，当没有大量的人在那里提供人群掩护或见证时，警察可以很轻易地围捕黑群团队。所以，不要在你们的汇合点上磨蹭很久—— 要及时，所有人要守时，汇合后立刻开始行动。

某些时候出现这样的情况：一旦聚集起来，黑群就很难进入行动区域了，因为那里已经布满了警察；于是在大规模行动中，最好的选择之一是让黑群团队绕开警力密集的区域汇合，然后融入到更大的团体中再进入该地区（如果您真的需要去那里的话。也许您应该考虑在另一个方向可以完成什么？），然后再分开作为一个“群”行动。当与其他人一起行动时，一个黑群应该与周围其他人保持紧密联系，并在团体内部保持紧密；因为警察可能会尝试隔离黑群成员。

[image]

一旦聚集在一起，在空间上要保持紧密（侦查小组显然是个例外，他们需要在更远的地方）—— 您需要把警察挡在您的队伍之外，因为警察经常试图拉走个人；也要把您的朋友留在您身边，而不是让陌生人或可能的卧底在您身边。横幅（用PVC管加固，或者更好的是，只要您能把它们安全地带到街上，用坚硬挺括的绝缘板制成的大标语牌，上面装有手柄，会更好；这些可以绑在一起或用链子拴住，形成一个移动的、联合的全尺寸路障）在一个前进中的团体的前面和两侧可以提供保护。

[image]

请记住，是行动者们的实际存在和团结构成了你们的力量，

你们能为击退警察的指控和挫败逮捕的企图所作出的准备就是你们的前进许可。

如果你们在警察不准备进行大规模逮捕或用化学武器攻击时出击，警察就会通过随机对个人进行攻击或逮捕来恐吓你们所有人；

尽可能阻止这种情况发生，彼此互相保护，不要退缩。

有可能的话提前在一个地区隐藏有用的材料—— 垃圾箱里可以装上

树枝和石头或喷漆罐。敏感材料（如射弹）可以藏在玩偶里运到行动现场，用普通的装饰品或纸箱子盖在可能的盾牌上。请记住，如果您被逮捕，身上携带着一袋石块、瓶子、汽油等物品绝对不会是好事。不要忘了，只要有一个简单的工具，总是可以当场把混凝土或沥青打成弹丸。

在计划和行动期间，你们小组的每个人都应该有一个一次性的绰号，这样你们就可以在不泄露身份的情况下互相称呼。那些通过手机或对讲机进行通信的队友必需假设警察正在监听；学习某种暗语可能是明智的，或者至少牢记不能在这种情况下说什么。

对于一个亲密团队或黑群来说，提前学习暗语编码的公告也是很好的，这样你们之间就可以在无关的人不明白什么意思的情况下公开进行交流。请记得，只在必需的情况下使用暗语；笨拙地使用暗语实际上会使您处于更大的危险之中，因为当局可以声称您的暗语代表了比实际更严重的事。另外，不要害怕向大家发出无暗语的通知，比如："不要惊慌，团结起来！"，"我们需要靠近并填补这里的空间，在前面放慢速度！"，"医务人员！"，"谁能证实他说的话？"，"保持队形！"

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

[image]

在激烈的行动中，您在亲密团队中建立的所有结构都很容易被解散，比如个人在现场被新的形势发展所吸引。不要失去理智，不要盲目；确保在空间上始终与您的团体保持紧密联系，与他们保持沟通，了解正在发生的事，保持您的角色不要分心。有一个非正式的队形可能会有帮助—— 比如，您可以一直在某个同伴身后几步远的地方，另一个朋友始终在您身边，还有一个朋友在您身后。计划会发生变化，但不要失去使你们能够统一改变计划的结构。

不要惊慌，不要相信未经证实的传言。在行动期间，您可能要到第二天才能清楚地知道其他地方发生了什么，如果有的话；在这一切之中，很容易被一波又一波的错误信息所冲击，所以在您仔细核实之

前，不要对任何传闻采取行动。更不要自己散布谣言，也不要只告诉别人您根据所看到或听到的传言推测出的结论 —— 要直接告诉其他队友您看到或听到了什么，让他们自己去得出结论。

侦察小组应该练习在不显眼的情况下使用通讯设备，如果适用的话，在骑自行车的时候使用通讯设备的技巧也要练习；那些被认定为侦察员的人很容易被警察骚扰，这将是更大的问题，因为他们是远离大部队独自行动的，他们对团体的成功至关重要。他们应该特别迅速和警觉。使用无线电的侦查员应确保彼此事先共同决定好使用的频道、暗语等细节，并在出现问题时有一个备用频道。

[image]

路障可以用任何东西制成，可以起到减缓警察的进度或简单地阻止交通的作用；如果您提前侦察过，应该能够做到在混乱的人群中也可以很快将路障安置好。千万不要完全封锁您可能需要的逃生路线。在对抗性不强的情况下，您可以通过简单地在单行道上走错路，使警察更难以有组织地跟踪您，但前提是仍有车辆从那里过来。

攻击性地使用投射物是很严重的事，如果被逮捕，可能会被关很多年，但这种战术可以让警察保持距离，以保护一个地区、或者激起镇压者使用催泪瓦斯（实际上这可能是警方希望避免的一种战术）。不要在一个可以被包围的小团体中开始投掷石头等 —— 留待大规模冲突时再使用，在这种情况下，城市在一个方向属于警察，另一个方向属于抗议者。当您投掷时，作为大团体的一部分，从人群的前面投掷，并在有争议的地区保持稳定的呼声。投掷者身后的人可以通过水桶传递提供更多的石块。

如果您的行动打算进行财产破坏，请配备适当的工具。确保您了解您的目标和这些目标的弱点或力量；如果已到现场却发现此处安装的是无法被打破的防碎玻璃，您就白白冒了很多风险。有时，喷漆可以比碎玻璃更有说服力。在被打碎的公司大门喷上标语，人们会很想拍摄的 —— 当然，如果可能的话，您也可以直接在他们的监视摄像头镜头上喷漆。

[image]

返回：[image]“不要再拍了！请关闭设备删除影像”

返回 - 自卫措施：[image]反攻

[image]

在街头对抗中，您可能应该考虑使用的最危险的武器是燃烧瓶。使用燃烧瓶的人可能会遭到警察的严重报复；只有当在您身后有一个没有警察的区域，而且附近有同情的人群，您可以逃到那里而不会不必要地危及任何人时，您才应该使用这种战术。

最好的情况是，您和队友融入在一大群愤怒的人中，使用燃烧瓶，然后迅速消失。如果可能的话，尽量将投射目标瞄准财产，而不是警察。

最好向警察扔漆弹（可以用玻璃瓶、灯泡、空心圣诞树装饰品或装满油漆的蜡球制成），或用弹弓射出漆弹。如果警察的头盔和盾牌上沾上了油漆，虽然不会有任何人受伤，但他们很可能一定程度地撤退。

有各种各样的警察武器可能被用来对付你：胡椒喷雾、催泪瓦斯、水炮、闪光弹、橡皮子弹、棍棒、冲锋马或车辆，您需要知道在每种情况下会发生什么，并做好相应的准备。有时，好的进攻就是最好的防御；一个准备好的黑群比警察所预期的更快、更勇敢地行动，可以在水炮被用来对付抗议者之前使其失效。催泪瓦斯榴弹可以扔回给警察，但它们落地后会非常热；如果您打算这样做，请确保戴上焊接手套或其他有效的防热措施，并确保您有足够好的投掷水平。在榴弹开始释放气体之前，不要把它们捡起来—— 它们可能会爆炸并伤到你。马匹可能会对接近着火的地方望而却步；对抗性不强的群众也可以通过全部坐下来或躺下来阻止马匹冲锋。

[image]

当警察不准备大规模逮捕人们时，他们会努力驱散抗议人群。

如果群众看起来特别喧闹，警方可能先使用催泪瓦斯、震荡榴弹、橡皮子弹等；然后，当警察认为“安全” 时，就会进入这一区域。

他们可能会排成一排，冲锋和后退，在再次冲锋之前重新组织和巩固

此前的成果。

在这个时候，除非面对警察的人群是紧密团结的，有路障保护的，或者是彼此手臂紧紧相连的，否则就会发生暴力的个人逮捕，以恐吓群众。

当人群看起来动荡不安、胆大妄为时，警察很可能会保持一定的距离；如果人群混乱、被动或凝聚力低，警察可能会在人群中形成阵势，以加快进程。

在任何时候，您都不应该惊慌失措地奔跑—— 那样做只能增加您冲进麻烦的机会，并在这个过程中危及其他人；如果其他人开始奔跑，就大声喊："走路，不要跑！" 同时，保持快速移动，保持混乱，以防止警察了解你们要去哪里或期待什么；永远不要让警察队伍在人群中聚集。

[image]

如果您在大街上，警察会试图把您逼到人行道上；这可以稀释人群，降低士气，并使您离被逼上绝路更近一步。如果您被逼到人行道上，您可以利用过街天桥或转到小街上，重新夺回柏油路；扛着横幅的人可以冲上前去，在人多的时候堵住准备占领的地方，骑自行车的人也可以。其他车道也是如此，如果镇压者努力将你们限制在你们所抢占的车道上。

如果警察不能让每个人都走上人行道，他们至少会试图吓唬人群中不那么激进的人，让他们走上人行道，扮演一个旁观者的角色，这样警察就可以专注于对付激进派活动家；在这种情况下，你们应该尽量保持移动和循环，这样被警方隔离出去的 "旁观者" 就可以再次被吸收进队伍，当然，如果您在连接紧密的黑群中移动，您不会希望在这种情况下失去凝聚力。

在城市环境中，一个有组织的、警觉的黑群有可能比骑警更快地徒步移动；始终保持移动并保持在你的敌人前面。突如其来的速度和方向的改变可以让警察特别困惑—— 只要确保您的团队可以有效协调地参与这些活动而不至于自己变得混乱或分裂。为了协调大团体的同步行动，您可以喊出从十到一的倒数。

警方的支援小队可以被派往人群中，抓捕警方认为是“头目”或 “危险”的活动家。有时您可以清楚地看到警方的指挥人员指出要抓谁（如果有警察发射橡皮子弹，也可能是这种情况—— 另一名警察可能为射击者挑选了目标，通过观察您也许就可以知道谁将成为目标）。

警方的支援小队将试图包围 “目标”，同时保持一条开放的出口以便回到警戒线。为了防止这种情况，要密切注意警察的动向—— 他们可能会在试图推入前形成一条与抗议人群垂直的直线。

[image]

如果您知道被警察瞄准的目标是谁，让此人迅速离开这个区域，换上不同的衣服。

把您的身体放在接近的警察和 “目标人” 之间；不断移动，阻挡警察的道路，同时尽可能让一切看起来很自然，这样就不会使您自己成为目标。

如果一群人能够隔离和包围进入抗议者人群的个别警察，后者如果感觉控制不住就会退缩。

另一些队员可以从警察手中重新抢回被抓的人。这样做的时机是警察出手后直到他们回到自己的防线之前。需要有几个人打破警察的钳制，其他人则阻挡警察的道路。

[image]

一旦您的队友得到解救，就把手臂连接起来，立即消失在人群中。警队可能会再次尝试抢人，而且现在他们也会瞄准其他未被捕者；

请记住，阻止逮捕可能会导致比原先所面临的更严重的刑事指控，所以只有在您有很大的成功机会或不这样做风险太高时再冒这个险。

以前曾发生过被愤怒的人群包围的警车被迫释放被捕者的情况，但这群抗议者也不得不被困在那里。如果警车的轮胎被刺破（刺破侧壁，

而不是胎面），这当然会迫使警察停下来，但爆胎的声音会很大——还是那句话，除非您融入在一个值得信赖的人群中，在足够的范围内有掩护，否则不要尝试这个方法。

[image]

如果被警察抓住的是您，请记住，即使是最温和的自卫也会导致攻击性的指控。

如果您预计您的同伴会试图把您抢回来，那就通过继续移动使逮捕您的警察的工作变得困难，否则就瘫软在地上：这不会导致袭警的指控（尽管某些时候会导致 “拒捕” 的指控），而且会迫使警察更努力地移动你。

请记住，瘫软在地上的方法可能会激起警察对您采取更多的暴力。但如果警察的每一次逮捕都要花费大量的人力和时间，那么您的朋友就会处于更有利的位置可以逃跑或试图救援你。

总是有这样的可能性，警察会完全包围你们整个团队，并逐一逮捕你们。如果发生这种情况你们就有麻烦了。最好的防御措施是通过侦察员及时了解警察的动向：他们可能会试图从哪个侧面的街道上来包围你们，或者他们会可能如何引诱你们的前进，同时派人围住你们，切断你们的退路。

[image]

如果您发现您的队伍被警察的阵线包围，而这些阵线在一个方向上很稀疏，您可以尝试从这里冲出去：用你们自己的紧密的前线，用屏障做保护（旗帜、盾牌、围栏、至少是连在一起的手臂都可以），作为一道坚固的“墙”来推进，可能在队伍的最前面形成一个冲锋尖端来分割警方的队伍。

一个黑群曾经采取从建筑工地上挪用的手推车作为冲锋的前沿，冲破了警察的防线。

在你们被包围后，在警方完全确定情况之前，尽快应用这种战术，如果您想让这种方法发挥作用，就要有最大的信心。

通常情况下，你们最好的撤离机会是 作为一个有凝聚力的团体全部在一起 ；这也允许您在这个过程中保留自己的装备和衣服，因此你们可以保持作为一个团队的有效性，即使只选择用它来逃跑。

另一方面，如果您正在和一群人进入一个您认为可能是陷阱的区域，在您进入那个您可能无法逃脱的空间之前，消失在人行道上并脱下您的黑群装备可能是最明智的。如果您无可奈何地被困住了，请确保在被逮捕之前扔掉所有可能被治罪的物品。

[image]

请记住，除非警察有很多手铐、足够多的面包车或公共汽车，否则他们无法进行大规模逮捕，所以这些观察可以成为一个很好的提示，让人们知道该怎么做。化学武器也是如此；如果警方准备使用催泪瓦斯，他们自己就会先戴上防毒面具。仔细观察。

想想警察的目标是什么，以及这些目标如何影响您的选择：如果他们试图保持游行路线或围栏区域的安全，您实际上可能在其他区域自由活动一段时间；如果他们试图将大规模的游行置于观察之下，他们将不得不分散他们的力量才能跟上分离的游行队伍；当然，如果他们在数量上没有足够的准备，这对他们来说才是最困难的，但在某些情况下，可能确实是10组50人比一组500人更有效。在突发事件中，警方会有原地待命的时刻；您应该利用这些时刻—— 但如果有一段异常长的时间没有警察活动，这可能表明镇压者有一个诡计，例如一支新的、更重的武装和装甲部队正在附近集结。

[image]

在当权者可以看到的行动中，您可能会受到便衣人员的监视，而且您可能还得对付挑衅者。注意周围的人，特别是陌生人；卧底可能很容易识别（他们往往是男人，成对出行，脸上有至少两天的胡茬，可能戴着漂亮的手表和通信设备），也可能非常难以识别。让您的同伴了解每一个您怀疑的人，但不要 “暴露” 卧底，除非您绝对确定他们是特工（例如，您的一个侦察员一直在跟踪一个人，看到他和他的同事聊天），而且可以从中获得一些具体的东西。

示威者之间毫无根据的指责只能使局势更加紧张、示威环境更加不受欢迎。至于挑衅者和普通的蠢货，他们可能在你们的队伍中间或附近

活动，打砸当地的商店和私人车辆；无论您是否能证明他们是警察或线人，您当然可以直接向他们表明，他们所做的事是不可接受的，必须停止。不要在行动中陷入战术辩论，只要表明您的观点即可（或者在最坏的情况下，进行干预），然后继续按计划做事。

除了警察之外，也要注意其他人；其他更 “自由派” 或更专制的示威者可能会主动干涉你们的活动，揭开你的面具，攻击你，或向当局指出你；当地平民也是如此。千万不要用暴力来回应这种情况；如果有必要，就走开，或者逃跑。如果直接行动演变成与当地人或其他活动人士的争吵，对每个人来说都是灾难性的。如果有可能和有价值的话，尝试在一个远离直接行动的安全空间里，在脾气冷却后，谈出分歧；必要时派一个发言人，最好是一个来自黑群团队之外的支持者。至少，这可以分散插手者的注意力，而小组的其他成员则可以继续进行其他行动。

[image]

返回 - 相关镇压手段：平民告密 ；渗透者

尽管事情变得很疯狂，但请记住，警察有枪，您很少有理由为行动冒着被杀的危险。与武装较好的警察在街头遭遇，几乎总是会出现一些对抗的场面。警察的所作所为受制于公众舆论对它的裁决；你们的所作所为也受制于类似的问题，因为每当你们上升到更多的对抗性战术时，警察就会立即将他们的战术提升到比你更高的水平上。

在这个意义上，街头斗殴对激进派活动家来说是一个骑士精神的问题：我们总是允许对手使用更强大的武器以防止暴力失控—— 当然也是为了炫耀我们是多么的高尚和勇敢—— 如果报纸上写着 “当活动家开始回击警察发射的催泪弹时，暴力就爆发了”，大家就会明白发生了什么。

[image]

返回：[image]街头搏击基本技巧（转帖）

[image]

在战术上保持灵活。如果你们穿着防暴装备出现在与警察的对抗中，

却发现自己的人数完全不够，而且没有准备好，你们可以转向另一个方向，在附近的社区捡拾垃圾，美化环境—— 这将给媒体带来混乱的信息。

再次重申，如果你们在示威环境之外运用黑群战术，这一切都会非常不同。与其与警察发生您希望会有感染力的对抗，或者至少冒着这种可能性，您应该尽一切可能避免与警察相遇。在这种情况下，侦察员的作用更多的是提醒你们注意警察的接近，而不是监视附近警察部队的笨重行动，因此，在高速公路立交桥上或在商店外伪装成路人的侦察员可能比骑自行车更好。

撤离

在行动结束时，剩下的最后一个挑战就是脱掉你的装备并消失。

穿衣的层次再次是关键：在您的黑群服装下面，应该穿着能够使您很容易与该地区的任何自由派抗议者或平民融合在一起的服装。您可能不得不在一瞬间脱下最外面这层衣服：例如，如果警察专门瞄准您并追捕您的时候。

确保脱衣服是一个快速和容易的过程。尽量在注意力不集中的人群中，或在拐角处或灌木丛中脱衣服；如果您被看到或被拍到换衣服，您所做的掩饰可能就白费了。

希望您已经计划好了一两条巧妙的撤离路线：一条不显眼的小巷，一个宽大到任何警察路障都无法阻挡的空地，一个您能够比任何猪警官更快爬上的栅栏。如果可能的话，您可能想在附近锁上一辆自行车，这样一旦您逃脱了，就可以跳上自行车快速离开那里；在城市环境中，也可以试着叫一辆出租车（只要还有出租车），或者上地铁（尽管在严重的情况下，地铁很可能会被关闭，或者警察会检查所有进来的人），或者躲进一家餐馆，在一个安静的角落里穿着您的平民伪装吃薯条，直到事情平息。

请注意，除非事情变得非常棘手时再这样做，否则您应该仍然和您的

伙伴在一起，不管是不是您的亲密团队的成员。

最后，所有直接行动的首要规则就是：在你领先的时候退出。尽你所能，但活着是为了能再战一天，除非今天真的就是最后一战。

[image]

事后

行动结束后，在安全地远离危险和监视的地方和时间，再次聚集在您的亲密团队中。给每个人一个空间来分享他们的感受。讨论和评论发生了什么，您从中学到了什么，它对未来意味着什么。如果适用，请确保向参与黑群行动的其他亲密团队报告你们的结论，并寻求他们的反馈。如果你们中有人被逮捕或面临其他困难，如受伤，讨论如何处理。庆祝你们的成就，彼此提供情感支持，如果有必要，可以发誓和策划回击行动。最重要的是，要确保每个参与者都知道自己是被爱的和受支持的。

永远不要吹嘘您在集体中的成就，也不要分享任何其他人不需要知道的事，特别是如果相关信息可能使某人入罪的话。请记住，无论您如何精心伪装依然有可能被拍到，会被当局发现。在瑞典，在欧盟的一次会议上发生街头对抗的几个月后，一天清晨，警察来到几十名参与那次活动的行动者的住所，并在同一时刻将他们全部逮捕。这是一个最坏的情况—— 不要让这种情况使您变得偏执。只要保持对危险的认识；如果您正在做很多繁重的事，或者正在组织这类事，您应该选择住在一个隐秘的地方，让您的敌人很难在任何特定的早晨找到您。

[image]

本指南中未涉及的一些重要的相关主题包括：

- 监狱团结和监狱支持
- 救护医疗

- 法律观察员
- 处理逮捕
- 咨询和支持

[image]

[image]
[image]

反击, 保持自由：街头实战指南 S05E17

[image] 关键词	一次性手机 亲密团队 免追踪 准备工作 匿名着装 协作 反渗透 团体团队 威胁响应 威胁模型 安全屋 安全文化 操作安全性 数据最小化 整体 直接行动 移动设备 空中监视 街头 街头战术 通信 防御 防暴武器
[image] 关联	[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训
[image] 创建时间	2025年1月20日
[image] **Description**	行动安全性

- 警方和特工通常如何识别并锁定参与示威的人？

- 我们能采取哪些反制措施来抵御此类镇压？

本文来自某个匿名的亲密团队，探讨了他们应对这些问题的策略。这是一份很专业的安防战术介绍。

- Table of Contents
把风险降至最低
示威行动准备指南
磨合方案
筹备全套装备
以下是选购一次性外层服装的头到脚指南：
洁癖是重要的安全品质

应对镇压与突袭的准备
小心你口袋里的警察
1、隐蔽地激活麦克风
2、定位追踪
3、数据提取（即数字取证）
在街头
成为无名者
在紧要关头做出决策
警方监视
其他形式的监控
其他威胁
铺路石下是海滩
所谓撤离，就是要消失得无影无踪
择日再战
应对偏执的最佳良方是现实主义和充分的准备

[image]

曾经，只有那些打算参与高风险对抗性活动的激进派人士才需要关注监控与安全问题。而如今，大规模的监控和警务正变得愈发侵入性与任意。即便您从未触犯任何法律，国家仍可能试图拿您当作典型案例杀鸡儆猴。所以，所有可能参与示威活动的人 —— 不论哪种风格 —— 都应该学习和熟悉激进派前线历经多年挫折总结出的安全规程。

如果您是街头新手，请不要被所有这些考量吓倒。参与街头抗争的人数越多，对所有人来说就越安全—— 而最危险的莫过于孤立消极地坐以待毙，任由警察国家逐个清剿我们。

本指南仅概述如何在抗议活动中最大化保障自身安全。

如果您需要更全面的背景知识，建议先了解如何组建亲密团队以参与示威、如何策划直接行动、以及如何在示威中穿着统一服装，等等，在下面看到；本专题 “行动安全性” 中应该已经收纳了大部分您所需要的知识和经验。

[image]

返回：[image]您需要真正的自己人-如何组成一个亲密团队：街头实

战指南 S05E09

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

武汉人民直接行动，推翻了水马以解除封锁。2022年11月27日 attachment:63bcd788-419c-4ab1-9e39-d63d427ba068:武汉-2.mp4 [image]

把风险降至最低

所有参与抗议活动的人都被建议戴上面罩遮住脸，这不错。不过穿着打扮只是您众多必须考虑的问题之一。通过采取一系列反制措施——经常被称为行动安全措施（opsec）——您就可以降低被逮捕和起诉的风险。

即便您最终仍被戴上手铐，周密实施这些防护措施也能帮您最大限度地减弱指控证据的效力。记住这句俗语：无痕迹，就无案底。

示威行动准备指南

[image] 一名示威者正在保护社区免受催泪瓦斯的侵害。请注意他在下蹲的过程中其腰部正在暴露，这是超出预期的。如果您的肤色有特征，或者腰部有疤痕或纹身，一个下蹲动作就会导致您被监视器识别身份。请务必提前穿戴全部上场服饰进行练习，选择那种能确保在任何姿势下都可以完全遮盖身体的服装。

磨合方案

每当我们的亲密团队聚会以进行准备工作时，我们都会尽量留出足够的时间来全面过一遍所有事项。

- 首先，我们的战术目标是什么？—— 通过这项行动我们想要实现什么；

- 示威活动将在哪里进行，关于地点我们了解哪些细节？ BACK [image]地形侦查 ；[image]监控侦测 ；

- 需要的东西都准备好了吗？谁负责带哪种东西大家记住了吗，准备如何把东西带到现场？ BACK 周密的行动计划 ；[image]匿名购买 ；

- 我们认识的其他人也会来吗？我们打算在哪个时间点以何种方式撤离？有人感到特别担忧或害怕吗？…… 等等。

示威活动既能激发众人携手行动的热情，也可能带来精神创伤。讨论“个人能力的极限”这个话题对亲密团队至关重要 —— 比如：是否有人身上有旧伤，导致不能跑得更快？是否有人近视却不能在呼吸器下面戴眼镜，导致影响行动中的机敏度？您对这片城区的街道有多熟悉？某些场景是否会因过往的经历而引发恐慌？

假装大家都没有恐惧、创伤或身体上的限制是毫无益处的。我们希望相互支持，这样才能共同发挥最大的效用。

在示威前的讨论中，人们往往容易以偏概全。就像这样：“那不常态么”；“警察肯定会这么做的”；“这绝对能奏效” ……等等。最好避免下定论，对可能发生的事情保持开放心态。我们应专注于厘清个人目标，确保在机遇出现时具备行动所需的一切条件，同时预判最可能出现的机遇。如果有人断言“这不会发生”，导致您准备不足，而错失良机，那种感觉会非常糟糕。

切忌过度规划。

我们追求灵活准备：思考行动方案并做好实施的准备，同时保持应对突发状况的弹性。实践表明，耗费数小时讨论往往收效甚微 —— 事态发展常与预期大相径庭。我们讨论的并非深夜小规模行动（这类行

动可精确规划），而是涉及众多参与者的、充满动态变数的大型示威活动。当然，熟悉地形至关重要：能帮助您发现有趣的路线，并避开警方的封锁围堵。

[image]

某些示威活动设有预定路线，此时提前踩点尤为重要 —— 需勘察换装点、物资集散点及撤离通道。务必标记监控盲区、死胡同、瓶颈路段及潜在突破口。

但也不要准备不足。

不要理所当然地认为会有人带头行动。如果您想让某事发生，您可能就是需要挺身而出的那个人。同理，物资包闲置总比关键时刻缺失必需品更可取。

如需携带可能引发不当关注的工具或资源，且集会点存在被安检的风险，我们就将在游行启动后再加入 —— 待警方将注意力从外围监控转向人群管控时。

如果无法预知游行路线，负责运输物资的人应该骑自行车进出 [image]自行车接力 ；此举亦可缩短暴露于警方侧翼或尾随视线的时间。沿途藏匿物资虽可行，但当游行路线突变时就会屡屡失效；如今我们更倾向其他方案。

深入分析当地警方战术的演变至关重要：当地防暴队训练是否到位？是否常采用“水壶战术”封锁所有出口实施大规模逮捕？是否针对性打击示威集结点？使用何种催泪瓦斯及何种情境下使用？何时动用橡皮子弹？…… 还能识别哪些行为模式？

当地警方通常会研究示威者的战术并制定应对策略。这些策略还会因警力配置、资源状况及其他因素而变化 ——例如政治或法律环境的变化可能使某些人群控制手段变得不可行。威活动本身就具有不可预测性，因而难以预判警方在特定日子的部署方案，更不用说应对突发状况时的反应了。所以我们力求从宏观历史视角展开分析，重点探讨镇压策略如何随情境变化而调整，而非简单的追问“上次发生了什么”并

期待历史重演。

要想采用更系统化的规划方法，不妨试试“威胁建模”——分析对手的能力与动机，反思自身可能存在的脆弱点，据此制定既能降低风险又能实现目标的应对策略。在下面看到练习。建议参考威胁知识库及其教程，该教程专门以激进派直接行动的背景探讨威胁建模的实践。

[image]

返回-练习：[image]S01E05-T3 确认可能遭受的所有威胁

返回-练习：[image]S01E05-T4 态势监测和威胁清单

返回-练习：[image]S01E03-T2 绘制行为者关系图谱

返回-练习：[image]S01E06-T2 找到弱点建设新的防御能力

返回：威胁知识库-索引页

返回 - 一个重要的演示：[image]带有攻击树的威胁库用例示范

需要强调的是 —— 如果是以小型团体的形式策划行动，应聚焦于实现一两个具体的目标，其余环节保持灵活。如果是要基于一系列无法掌控的变数制定复杂的计划，结果可能与预期相去甚远。如果计划缺乏弹性空间，明智之举应该是执行既定方案后全力确保安全撤离。通过出色完成预定行动，您可能已经为他人创造了实现目标的契机。这就是成功。

[image] 2019年五一节，万隆市黑群示威活动。摄影：弗兰斯·阿里·普拉塞蒂奥。

筹备全套装备

执行计划所需的一切物资都需要花钱：[image]手套 、新衣物、材

料、交通及其他开销。我们力求在成员间分摊成本，确保无人承受经济压力。

所有采购均使用现金支付，敏感物品提前购置，分散在不同的店铺购买，穿着保护隐私的衣物（比如帽子和N95口罩）。对于每件重要物品，我们都会预判警察可能追溯的购买路径，并清除所有相关序列号或射频识别标签。

[image]

相关自卫措施：[image]匿名购买 ；[image]匿名着装

参与黑群行动时所有暴露在外的衣物均视为一次性用品。有人穿着私人雨衣并用胶带遮盖商标，但我们认为这不足以保障安全。如果特定服装在高风险行动中被使用，那将是这件衣服的最后一次亮相。

我们竭力消除服装上任何可能暴露身份的特征。有时用黑色记号笔覆盖标识或拆线即可，但更理想的做法是直接选择无标识的服装。宽松的服饰能有效隐藏身体轮廓，因此更受青睐。

以下是选购一次性外层服装的头到脚指南：

1、遮盖眉毛的黑色面罩。

可选方案是将透气面料（如棉质）旧T恤改制成面罩，通过系带完全遮蔽眉毛和鼻梁上部。

平角内裤亦可替代。

另一方案是在透气式头套两侧缝几针缩小眼部开口。

2、普通款黑色墨镜。

如果您不戴眼镜，警方摄影师就可以拍摄出高分辨率眼部照片、并识别肤色。

为防镜片起雾，需提前喷涂防雾喷雾。

可根据需求替换为：防催泪瓦斯喷雾时选用深色泳镜，面临橡皮子弹威胁时选用防撞护目镜。

必要时可配戴处方太阳镜或泳镜，因接触化学武器时不宜佩戴隐形眼镜。

夜间行动需选用浅色镜片太阳镜，务必提前在实际使用环境中测试装备的性能。

3、一件不起眼的黑色连帽衫或夹克。

如果当地警方使用彩弹/漆弹弹药标记示威者，可穿戴可脱卸的黑色外衣作为防护层。

防水衣物（如雨衣）最适合此用途，因其能阻隔标记染料渗透至内层衣物。

4、一双黑色手套。

我们推荐掌心采用光滑橡胶材质的劳保手套，其特点是不易撕裂、掌面防水且灵活度高、抓握力强。

但需注意：光滑橡胶手套外侧可能残留指纹，甚至转移到接触物体上；行动前务必清洁手套，穿戴时避免在外侧留下指纹。替代方案是使用布质工作手套，但其灵活性可能受限。若需接触催泪瓦斯罐（警方部署后罐体会持续高温），务必使用耐热手套。

[image]

相关自卫措施：[image]手套 ；[image]匿名着装 ；[image]DNA最小化方案

 2022年郑州工人反封锁起义，很棒的合作。可惜没有戴手套。
attachment:bd58e5b8-8cd2-4d62-b982-b3edaa3e06c5:2.mp4

5、一条普通黑色牛仔裤。

为更好地隐藏体型特征，可选择在牛仔裤外叠穿：a, 黑色可撕开式运动裤（便于快速脱卸）、b, 家居裤（更易获取，可在脚踝处开小口便于脱下时无需脱鞋），或者 c, 雨裤（更耐抗彩弹弹药）。

借鉴智利无政府主义者的做法，在鞋上套一双大号黑色袜子。多起案例表明，未采取此项额外防护措施的人导致鞋子的特征成为法庭上的主要证据。

袜子尺寸须足够宽松，能轻松套在鞋上。为便于快速脱卸，可用剪刀或刀具在每只袜子的脚踝处剪出两道一英寸长的开口——一道沿脚背，另一道沿脚背对侧；此举将使袜子前端翻折形成“舌状结构”，可抓握此处迅速撕脱袜子。

[image] 把旧T恤改成面罩的方法

根据示威活动的频率，如果每次都要单独准备服装很可能会耗费大量精力，因此我们通常会批量购买每种服装，然后将尚未用到的衣服存放在可信赖的朋友家中。

[image]

相关自卫措施：[image]匿名购买 ；[image]藏匿点或安全屋

打包示威装备时，我们遵循“最低负担”原则，这跟[image]信息最小化原则 类似。最低负担指的是：一旦有人被捕，随身物品可能会对携带者或他人造成危害 —— 比如示威传单，可能被用作证明当事人“蓄意参与”的证据，钱包里的东西可能为警方提供大量新线索，而日程本可能暴露人际关系信息 …… 因此除衣物和行动专用的物资外，我们坚持极简原则。

我们的标准是携带一张身份证件以备被捕或受伤时使用，另外备水及若干能量棒等轻食。若需服用日常处方药，可携带少量药瓶以防被捕。

同时务必准备足够的现金用来支付出租车或公共交通费用，或用于事后在咖啡馆、餐厅等场所融入环境。

如果当地拘留所环境需要，可携带硬币以备被捕时拨打电话。

[image]

除此之外，请将所有物品留在家中。仔细检查口袋和包袋，清除传单、收据小票、杂志、笔记等杂物。

即便不考虑被捕也要知道，任何携带物品都可能在混乱中遗失，后续拾获时就很可能被追溯关联到您本人或合作者。

这是一个关于如何把T恤改造成面罩的演示。您也可以使用平角内裤或其他普通贴身衣物达到类似效果。与视频中的示范不同的是，强烈建议您务必确保口罩能覆盖眉毛。
https://youtu.be/7tYzl9QXvkc

洁癖是重要的安全品质

示威活动结束后，警方的取证团队通常会搜寻现场和沿线以及散场点附近遗留的衣物和工具 —— 因此对行动者来说，在处理、存放和运输任何物质材料时请务必谨慎。

我们绝不直接用手触碰任何计划带走的工具，确保物体表面不留[image]指纹 。从一开始就避免在物品上留下指纹远比事后再用丙酮擦拭更有效，擦拭对某些表面来说效果是有限的，例如金属表面留下的指纹压痕，必须使用砂纸等研磨材料才能清除。

某些情况下，确保物品不沾染人类DNA 至关重要。皮肤细胞、毛发、唾液、血液和汗液都是DNA来源 —— 与指纹不同，一旦物体被

沾染DNA，就无法可靠地清除。

一个良好的起点应该是在接触物品前戴上全新的没有渗透性的[image]手套（即橡胶洗碗手套，而不是棉布等材质的手套），且穿戴时要小心避免光手触碰手套外部。

DNA法证技术的应用概率似乎与特定司法管辖区的检测成本呈正相关。部分地区已建立法证实验室，即使调查轻微犯罪也能采集DNA证据，尽管在一些国家，示威活动现场的DNA检测尚未成为证据采集的常规手段。

如果在可移动物体上发现DNA，其关联者可能数周前就接触过该物体，因此相较于在固定物体（如破碎的窗户）上发现DNA，前者情况对证明现场存在性说服力较弱。穿着衣物时无法避免留下DNA痕迹，因此在考虑DNA取证时，我们务必确保不要在现场遗留任何衣物。

[image] 请注意，这位智利示威者将袜子套在鞋上以遮掩鞋子的特征，同时竭力保护社区免受水炮的袭击。然而令人费解的是，他们居然没有戴手套，而且他还穿着印有醒目图案的运动衫，在监视器眼中这是明显标志性的东西。

应对镇压与突袭的准备

[image]

相关自卫措施：[image]镇压应对措施 ；[image]突袭应对措施 ；[image]防篡改准备 ；[image]物理入侵检测 ；[image]被捕支援 ；[image]藏匿点或安全屋

准备工作中至关重要的一环是制定最坏情况的预案。

镇压打击最猛烈的状况经常是在人们毫无准备之时。如果您突然被警方拘留，却不知道谁可以做您的律师、谁可以帮助照顾您的狗、谁会通知您的老板帮您请假、谁会支付您的保释金 —— 这种处境堪称煎熬。

我们集体筹备每一次的示威活动时，都要假设可能至少被关押一夜—— 例如预先聘请律师并牢记其联系方式，这都是最基本要做的准备。

听起来可能有点情绪耗损，但实践证明，这些准备恰恰能赋予我们更自由的行动力。

其他准备措施包括：把备用的房屋钥匙交给可信任的人、安排好子女或宠物的照料、指定保释金或房租支付人、把合作的电子邮箱及集体社交媒体账号的登录平局转交给值得信赖的亲密队友，等等。

另一个关键问题是：您需要假设在您被拘留的过程中，如果警方搜查您的住所寻找证据，他们是否会发现有助于他们构筑案件的任何物品？当然，每个人都需要结合自身情况回答这个问题，但必须牢记的是，突袭搜查何时发生、警方搜查的目标是什么，都无法预料。因此，我们应确保家中尽可能不存放任何可能引起检察官兴趣的材料。

[image]

基本原则是：切勿在家中存放特别敏感的物品。问题往往不止于单个可疑物证（如监控画面中出现的衣物），更要避免形成所谓“可疑物品集合” —— 例如烟花爆竹、弹弓、过量的同类衣物（手套、面罩、黑色连帽衫）等物品，均不宜存放家中。

敏感物品当然需要存放。可选方案是寄存于可信赖的且不易遭搜查的朋友家中——但需要注意的是：为避免物品组合显得可疑，建议将不同物品分散存放于不同地点或不同朋友的家中。

另一种方案是将物品藏匿于户外无人会偶然发现的[image]藏匿点或安全屋 中，且需确保取用时不易被察觉（例如深埋于远离小径的森林中，或藏于废弃建筑的天花板夹层中）。

至于家中存放的物品，我们绝不会将其摆放在“展示”架上，而是归位存放 —— 例如将密封包装的手套与家用清洁用品放在一起，放在厨房卫生角，而汽油放在车库里，鞭炮放在孩子的玩具柜里…… 等等。对于家中出现的任何物品，我们的律师都应该可以提供令人信服的正

当理由。

[image] 2019年智利的示威者。

小心你口袋里的警察

[image]

相关自卫措施：[image]匿名手机 ；[image]数字技术限制和最佳实践 ；[image]计算机和移动设备取证 ；[image]移动网络运营商 ；[image]数字取证 ；[image]户外无设备对话 ；恶意软件

[image] 2022年11月29日

警方调查人员常通过分析嫌疑人的手机和电脑使用记录来构建指控证据。

过去十年间，智能手机依赖文化已经在全球社会常态化，这极大的便利了条子们的工作。另一方面，尽管政府曾经可以远程监控未加密的语音通话和短信，但随着Signal等端对端加密通讯应用的普及，这种监控已经变得至少更加困难。而主要的威胁正在以其他形式出现。

[image]

返回：[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

当今手机监控主要涉及三大领域：隐蔽地激活麦克风、定位追踪、及数据提取（即数字取证）。

1、隐蔽地激活麦克风

[image]

相关镇压手段：□恶意软件

其中隐蔽激活麦克风虽然在新闻故事里最受关注，然实则发生的概率相比下最低，因为这种手段对镇压者来说需要耗费的资源最多 —— 要做到远程隐秘激活麦克风把手机变成窃听器，就必须先让目标手机感染某种恶意软件，这通常意味着目标设备必须被精准锁定并且有效感染病毒。就像卡舒吉的亲密朋友遭受的那种攻击。

杀死卡舒吉对沙特政权来说“值得”耗费以色列“飞马”间谍软件的巨额成本，而现实中多数情况下的你我都不是这个“级别”的反贼。

不过话说回来，随着语音智能家居产品越来越多、生物数据变得更加值钱、以及存储技术越来越便宜，如果您也像我一样有洁癖，还是建议您进行任何敏感对话时先确保身边环境中不存在任何所谓的智能设备 —— 包括智能手机和家居等等一切。平时选购时也尽可能不要买那种语音控制的和联网的小电器。

[image]户外无设备对话 是一项针对敏感对话的安全措施。我们希望您将这项措施在日常中作为卫生习惯来实践，以便增强防御直觉。

[image]

返回：[image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击

返回：[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

返回：[image]夸大危险并无助于解决问题：整体安全S01E04- 充分剖析您的信息资产

2、定位追踪

[image]

相关镇压手段：🔎 定位追踪

至于定位追踪，手机连接基站时其位置信息会自动上报给运营商，且该数据可追溯调取。警方只需掌握目标的手机号码，就能快速绘制该手机的历史移动轨迹，轻松呈现特定时段（如过去一年或示威前一周内）的活动模式与关联网络。

如果有人被捕，即便是最笨的条子或检察官，也会直接想到先询问当事人被捕前与谁同行、身处何地。手机自动定位功能使这类信息唾手可得。

任何可能成为调查对象的人都应该知晓并牢记这件事：日常携带手机出行很大程度上只会帮助条子掌握您的组织的大致联络对象，为连锅端打造基础 —— 因为分析哪些手机长期处于近距离接触状态是轻而易举的。警方尤其关注会议参与者的身份 —— 如果与会者均携带手机，即便事先关机，仍然可以轻易锁定在场人员。

[image]

抵御定位追踪的唯一方式，是彻底改变随身携带手机的习惯——不仅在敏感会议和示威活动时，更要养成定期将手机留在家中的习惯。

让社区集体践行此安全措施并抵制主流惯例 —— 例如提前制定计划而不是依赖持续的数字联络 —— 个人层面的行为改变就更易实现了。

3、数据提取（即数字取证）

[image]

相关镇压手段：[image]数字取证

关于数据提取，如果被警方获得了手机的物理控制权，我们必须假定

必然会发生数字取证。

逮捕行动通常伴随搜查令没收所有手机和电脑，且全世界众多警局都与以色列**Cellebrite**这类公司签约，该公司专门开发绕过磁盘加密的技术。

2024年7月泄露的文件显示，Cellebrite能解锁几乎所有安卓和iOS设备（我们推荐的安全版安卓系统GrapheneOS除外）。

[image]

需特别注意的是，**Signal**等加密通讯软件并不能解决根本问题。没有任何手机应用能真正实现消息从存储介质中“消失”—— 除非彻底格式化整个驱动器，否则取证专家总是可以恢复数据的。如果想要了解警方关注的手机数据类型，可参考J20抗议活动被告的证词（其手机曾遭警方扣押）。

谨慎使用手机固然不便，但身陷囹圄的代价更为沉重。只要您视手机为不可信设备、尽可能将其留在家中，手机监控的广泛可能性便不再构成威胁。随身携带手机会对您接触的每个人都产生安全隐患。

每次在手机上输入任何内容时，请预想这些文字终将在法庭上被朗读。

[image]

所有真正敏感的对话都应该当面进行，并且选择在户外场所进行，参与对话的所有人都应该把手机留在家中。遵循 BACK [image]户外无设备对话 原则。

手机仅适用于交换非敏感的信息或安排会面时间，绝不可用于任何可能被解读为“共谋”证据的沟通。若某项计划/行动需要远程联络，请考虑使用匿名购买的“一次性手机”或对讲机。

BACK [image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

每当我们不得不使用数字技术处理敏感事务时，我们仅使用**Tails**操作系统 —— 这款基于Linux的变体系统通过USB启动运行，不会在计算机上留下任何痕迹。

请注意：计算机唯一值得信赖的磁盘加密方案必须基于Linux操作系统 —— 由于Windows和macOS的源代码未公开，无法排除其存在后门程序的可能性，且安全研究人员已多次破解Windows磁盘的加密机制。

在街头

[image] 2017年2月1日，加利福尼亚州伯克利市的示威者。

成为无名者

[image]

相关自卫措施：[image]匿名着装 ；[image]监控侦测 ；[image]反监视 ；[image]地形侦查

当黑群组织形成时，参与者通常在示威集合点附近换上统一的黑色服装。

人们先以便装进入区域，换上黑群服装后加入队伍，结束后再换回便装离开现场。

[image]

为确保没有人能将您的“便装”与“黑群服”关联起来，这两次换装过程必须避免被警方、记者、或任何其他可能危及您的自由的人员记录或目击。

基于相同考量，开始换装时应立即完成整套更换，避免混搭两种装束

的中间状态。他人只能看到您身着便装或黑群装束，绝不能看到两者混合的状态。

即便穿着便装，也应尽量保持难以辨识的特征 —— 普通款N95口罩加帽子既能有效保护身份，又不易引起过度关注。

黑群行动者不必在集合点换装，可在行进中完成变装，这能有效阻断警方拍摄换装过程。在大型人群中实施此法更为便捷 —— 用周围人的身体彼此掩护。

我们选择远离警察视线、监控摄像头和拍摄手机的最佳地点更换服装。

理想位置是远离警方重点监控区域，但应距离汇合点足够近，可避免途中被拦截。

如果没有更好的选择，则深入人群中心，在横幅和雨伞后方蜷缩着更换。

尽可能选择能遮挡无人机视线的遮篷、天桥等遮蔽处更换服装。某些情况下，警方会专门安排人员进行人脸识别，条子们可能耗费数小时调取所有监控录像。建议所有参与行动的人提前演练穿脱行动服的流程，以提升效率并减轻压力。

只要我们的装束发挥其应有的作用，警方就应该更难区分具体个人的身份、难移追踪特定人员的行踪，也很难在法庭上提供有说服力的证词。

更换完毕后，我们要迅速互相检查，确保没有头发、眉毛（理想状态下）或皮肤暴露出来，没有“日常/平民”的底层衣物显露，且没有疤痕、穿孔或纹身等细节外露。

携带物资时，我们通常选择素色黑色手提袋而非其他时尚包包，因为后者更容易辨识。

某些背包可以穿在连帽衫里面，能有效压缩体积，这有助于收纳暂不使用的装备（如备用的衣物）。

如果需要使用防护装备（防弹衣、头盔、防毒面具及护目镜），黑群成员应该提前集体确定统一的型号——即便装备存在辨识特征，也至少无法仅凭此识别黑群成员的身份。

有时群体决定以“轻装阵” 形式参与示威，而不是穿着全脸遮盖的黑衣阵营服装。此时参与者不会全身黑衣，而是穿着灰色、棕色等暗淡色调的普通连帽衫或携带雨具遮掩脸部。此举旨在融入普通示威人群，因为警方更容易识别并锁定明显可辨的阵营。

然而一旦发生逮捕，相较于黑衣人示威者，“浅色服饰示威者”更容易被定罪。

[image]

穿着“不起眼”的衣服并不会使参与者难以辨认，示威现场的便衣警察、线人或旁观者更容易准确追踪他们目睹的采取特定行动的人，检察官也更容易确立目击行为实施者与后续被捕者之间的可信关联。

穿着无标识的黑色服装，使其与多数人穿着几乎无异，无论通过证词还是监控录像，都极大增加了建立这种关联的难度。

黑色服装难以与其他黑色服装区分，而彩色服装则存在明显色差。

黑色作为最强的光线吸收色，也使得身体特征及口袋、衣摆等细节在视频中更难辨识。

基于这些原因，当参与人数足够形成视觉冲击时，我们通常倾向于统一穿着黑色服装。全黑着装的逻辑不言自明，因此这种策略极有可能在街头广泛传播。例如在费城抗议活动中——当时一名杀害埃迪·伊里扎里的警察被撤销指控 —— 有报道指出，蒙面者和起义大军绝大多数人都身着黑色衣物。

上海乌鲁木齐中路抗议现场据说有一位英雄姑娘，帮助了其他行动者免于被捕。令人钦佩！上海的抗议现场似乎出现了围堵，这是镇压最常用的方法。这提醒了事先勘查并熟悉撤退路线是非常重要的。但如果您没来得及这样做，在这种情况下尽可能减少被捕的方法是：大家紧紧靠在一起，手拉手，站在外圈的人持有盾牌，围成一圈将人群裹住，逐步推进（不携带武器可以理解，但不携带护盾会很危险）。如果意识到警方正准备使用武力，以最快速度冲出包围圈才是明智的！请随时记得，团结是最强大的护盾。
attachment:935d15e0-f9b7-4dc5-bd08-572c90588105:6CJ5FwGCOB6LIGVH.mp4
[image]

在紧要关头做出决策

当时间紧迫且压力很大时，集体决策往往困难重重。在筹备会议中，我们力求充分讨论各项提案，确保每位参与者都有机会阐明立场 —— 但在示威现场这并非总能实现。

[image]

因此我们确保每个人都配有一至两名全程结伴的同伴，以便在更小、更灵活的小组中做出时效性决策。

通常无法判断在正常听力范围内是否存在便衣条子，因此我们规定在示威活动期间禁止使用真实姓名称呼彼此。我们会选择临时的（仅限一次性使用的！）团队代号，在混乱时刻需要重组时用代号呼叫队友，或作为全体联络的信号。必要时也会创建临时代号识别身份，不过通常只需简单指认即可。

避免恐慌和谣言传播至关重要。我们尽量避免依据未经证实的信息做决定，而是基于直接观察 —— 例如关注警方装备、人数和车辆的动态，而非在局势紧张时妄下最坏的推断。传递信息时，请描述亲眼所见（比如“我看到前排警察戴上了防毒面具！”），而非推测性结论（比如“他们要放毒气了！”），让信息接收者能基于事实自行判断。

[image]

报告亲眼所见时，可采用**SALUTE**协议 —— 即：规模/力量、活动、位置与方向、制服/特征、观察时间日期、装备；或**ALERTA**协议 —— 活动、位置、装备、所需响应、时间日期、外观，以便最大化信息传递价值。

示威活动节奏往往极快，这使得人们难以进行深思熟虑的沟通，这种环境下有时会导致伤害性或令人沮丧的互动。这类情况在当下处理起来会相当困难，尤其考虑到每个人对压力情境的反应各不相同。以我们的经验来看，最好是在行动后的总结会议中处理此类动态关系。

通过减轻压力以增强身心健康并减少人际关系负面影响，相关练习详见[image]S01整体安全 - 总章节：前线安防入门课 。建议每个亲密团队都应该学习压力下的情绪管理和神经系统调节实践，并将这些方法融入到街头行动的常规中。

警方监视

[image]

相关自卫措施：[image]监控侦测

相关镇压手段：[image]视频监控 ；空中监视 ；公开监视 ；[image]隐蔽监视

便衣条子可能试图渗透到您的群体中，尤其是在大型黑群阵营中 —— 因为这样的阵营中没有人能识别所有成员。

如果他们真的这样做了，其目的很可能是：观察高风险行动参与者、记录其更换衣物后的着装特征，并在游行散场后联合周边警力实施抓捕。数年前北美某城市示威现场曾发生示威者与便衣警察的言语交锋，结果后者随手就抽出了伸缩警棍。此后该市示威活动中，便衣警察要么以庞大阵容出现令人无法忽视，要么——显然——干脆缺席。原因显而易见，警察属于工会组织，即便高薪也难以说服他们冒险受伤，尤其考虑到便衣无法佩戴可识别的警用防护装备。

负责维持示威秩序的制服警察通常会进行某种形式的录像，且画面质量往往相当清晰。警方已经开始使用无人机对示威活动实施监控。他们通常会实时分析部分录像，以便在调遣警员冲锋期间或示威活动解散后（此时人群已丧失集体反抗能力）实施定点围捕。

[image]

如果您发现警察正指向某人（尤其是示威现场的指挥者），务必立即告知当事人。有时此举仅为威慑。

如果遭遇类似情况，当警察保持视线锁定时，更换衣物不会解决问题。

您不能在已经成为目标时换装，那是危险的。

务必确保安全脱离监视者视线范围后再更换衣物。

[image]

其他形式的监控

示威活动现场进行拍摄的人不只有条子 —— 公共和私人的监控摄像头、旁观者、甚至其他示威者，也都可能在拍摄影像。

乔治·弗洛伊德抗议活动中，许多参与者仅凭此类证据就遭到了逮捕并定罪。

[image]

拍摄高风险活动参与者的行为，无论您意图如何，在法律上都等同于上庭作证指控他们。

我们力图营造零容忍拍摄的示威文化（无论直播狂人、记者、还是手持智能手机的任何其他示威者），其灵感源自波特兰黑群组织 —— 在数起以这类证据为关键的法庭案件后，该组织致力于将此集体期望

变成严格规范并常态化。

[image]

返回：[image]“不要再拍了！请关闭设备删除影像”

摄像设备越早撤离示威现场越好，理想状态是在尚未发生任何可能被记录的事件前就撤离。

当您要求对方停止拍摄时，必须给予拍摄者收起设备的充分机会。参与者或支持者可在示威期间分发传单，阐明禁止拍摄的缘由。尽管部分直播者会顽固地继续拍摄，试图以牺牲他人自由为代价博取社交媒体关注，但多数人更可能根本没有仔细想过拍摄行为最终如何助长了警方的镇压力量。

无论如何，当有人被要求停止拍摄却仍继续时，划清界限完全合理。

与其陷入分散注意力的争执，更可行的方案是用涂鸦专用粗喷嘴喷漆覆盖镜头——这种喷嘴射程远，操作简便。

 中国郑州iPhone工厂工人抗议限制措施。请注意抗议者使用横幅推进的过程，这是很出色的表现。
https://t.me/iyouport/11898

遗憾的是，即便仅拍摄警方逮捕过程的法律观察员，仍可能增加拒捕定罪的风险、甚至导致更难解救被捕者。

阻碍警方行动的方式多种多样，完全不必依赖影像证据，影像这种东西更可能被权势用来对我们倒打一耙。路障、加固横幅、盾牌、雨伞、催泪瓦斯灭火器、激光笔、烟花、旗杆、灭火器、烟幕弹、铁蒺藜和油漆等等工具，都能有效阻止逮捕行动发生。请充分使用它们。

 泰国的抗议活动中抗议者阻止警方抓捕的过程。看起来似乎没有预先准备，这样被拖住是非常危险的。大家应该尽可能贴在一起，一起推进，避免被警方冲散。
https://t.me/iyouport/11874

即便是普通的布制横幅，也能通过遮挡摄影师视线以发挥作用。因此 —— 更不用说让横幅上的标语清晰可见了 —— 游行参与者不应在人群中央举旗，而应列队于队伍前后两侧，将横幅高举至足以遮蔽参与者身形、同时不阻碍其观察周边街道的那个高度。

[image] 不要拍摄！—— 即使是出于善意的摄影师，也可能对示威者构成威胁。 [image] 2022年11月中国的抗议活动中发生的事情

其他威胁

警察可能是您需要应对的最强大的威胁，但未必是最危险的。极右翼法西斯分子的行为往往更难以预测且更少约束。至少在美国，这有时会涉及驾车袭击或者枪支暴力。在2020年乔治·弗洛伊德抗议浪潮期间，为保护人群免受驾车袭击的伤害，部分城市采取了在示威队伍两侧部署车辆的常规防护措施。但这种模式存在明显弊端——既会延缓游行速度、限制行动自由，又很容易导致驾驶员面临法律风险。

针对枪击威胁，您应该熟知距离最近的且设有创伤中心的医院的具体位置、并制定抵达方案；请参阅以下内容了解示威期间应对枪伤的具体措施。参与示威时可穿着防弹护甲，但通常更重要的是保持环境警觉并随时做好快速反应准备。

[image]

返回：[image]如何处理枪伤：街头实战指南 S05E04

返回：[image]如何在大规模枪击案中幸存：反侦基础课 S06E09

返回：[image]了解防弹衣：街头实战指南 S05E08

示威活动中遭遇驾车袭击威胁或枪击的风险，可能与其他场景下的风险并无显著差异。如何应对示威现场的枪支问题衍生出诸多其他议题，超出本文讨论范围。

铺路石下是海滩

这是1968年5月法国起义的座右铭。

面对资源雄厚且擅长对称作战的对手，示威行动的核心优势在于机动性。防暴警察需负重装备，难以长时间持续小跑。其战术往往依赖短距离冲刺驱散或“驱赶”人群，随后便需停顿或撤入车辆；而警用车队则需要街道畅通无阻才能跟上示威队伍。

[image]

基于此，当警力冲锋时若我方人数占优，通常无需奔逃，更切忌惊慌失措。行进过快的示威队伍往往会不自已地松散开，这反而会使警方更容易锁定目标实施逮捕、或瓦解示威阵线。

与此同时，某些关键时刻少数人迅速行动至关重要。例如当少数警察试图列队围困示威者时，如果足够多的示威者能突破防线，警察就可能选择撤退而非冒险被包围。在德国，“五指成拳”的口号描述了多种战术 —— 涉及小分队突破警线后在另一侧汇聚成大部队。

从历史经验看，投掷物、烟火和路障能有效阻滞警方推进。如果您频繁参与大型示威，就肯定有机会亲见此类战术的运用。无论您是否参与其中，理解这些行动的本质与动机都是至关重要的。

当人群开始投掷物品时，必须向所有人强调：投掷物应仅从人群前方抛出。当投掷物越过示威者头顶时，极易造成严重伤害。同样，瞄准人群前方或侧方的目标投掷也存在风险 —— 即便瞄得狠精准，物体仍可能弹射击中窗户，导致碎片飞溅伤及旁人。防暴警察个个穿着昂贵的纳税人资助的防护装备，但示威者或路人可没有这么好的护甲，他们每个人都可以因为同伴的失误而遭受重伤。

我们目睹过示威团体事先收集投掷物，以便在冲突爆发时将满袋物品倾倒在人群与警察之间，让空手而来的参与者也能加入投掷行列。这是值得推荐的战术。

[image]

石头和锤子都能砸碎窗户，但各自涉及不同的安全考量。

石头用途更广泛；当不再需要时，只要置于合适的环境中，它们就比锤子更不易引起警方取证团队的注意。相比下在混乱或拥挤的场合，使用锤子可能更安全。

锤子可反复使用，且更易瞄准目标，对玻璃窗效果尤其显著 —— 因玻璃在边缘区域更坚硬，敲击窗角更易破裂。

如果有人用锤子砸碎窗户，玻璃微粒就会溅落到附近人员的衣物上，警方有专用的探照灯可检测此类痕迹 BACK 痕量证据鉴定 ；而石块则可以从足够远的距离投掷，避免产生此类痕迹。

使用锤子砸碎玻璃还存在割伤的风险 ——例如当玻璃破碎时，惯性可能导致使用者手部穿透窗框。而使用配重合理的建筑锤时，仅需手腕轻甩便能产生足够力量击碎多数窗户，同时保持手臂稳定远离玻璃碎片。

如今，银行、连锁企业及政府大楼越来越多地安装了昂贵且难以破损的窗户。这些玻璃可能采用加厚设计并夹层特殊材料，或是具有特殊弹性——这通常是聚碳酸酯板的特征。目前尚无简易方法识别此类强化窗户，我们建议勿传播所谓"某类窗户不可破"的误传。通常只需施加更大力量，或对同一角落多次击打即可破除。使用瓷器等高密度材料的碎块，其破窗效果可能优于石块。

燃烧瓶作为抵抗象征已经被神化了数十年。但一味的浪漫化可能带来危险的错误印象，会遮蔽实现中实现相同目标的情况下相比起来更安全且高效的途径。与原包装的助燃剂不同，燃烧瓶在法律上被归类为"简易爆炸装置"，这使得持有或使用该物品的量刑标准更为严苛。任何考虑制造或使用燃烧瓶的人，都应该仔细分析其中的风险，包括要掂量一下可能面临长期监禁的后果。

[image]

请记得，起义的规模越大，我们所有人就越安全

—— 当警察放弃对整个区域的掌控，转而专注于守卫固定的地盘时，

对我们来说，许多原本不可能的事情都会变得可能。

头脑要灵活，要保持敏锐和机动性。

所谓撤离，就是要消失得无影无踪

[image]

择日再战

关键在于认清警察何时成功重新掌控局面。当人群基本散去时，撤离或许是明智之举。此时是否回家取决于局势重燃的可能性，或者是附近是否仍有活动。

[image]

但应避免陷入"闲逛"状态 —— 即刚换下行动服的人群在某处游荡，被动等待刺激事件发生而不主动行动 —— 这是大忌。这种行为不仅为警方制造了更多抓捕机会，通常也难以取得实质性成果。

应该特别留意的是在脱下装备后的几分钟内是否有人尾随，以便在对方协调逮捕行动前摆脱他们。

我们判断威胁时并非仅凭对方是否像警察 —— 若警方稍有头脑，定会安排外表不像警察的人做便衣。相反，我们应该观察示威散场后是否有陌生人尾随。我们频繁变换行进方向，迫使追踪者做出同样不合逻辑的转向才能保持视线接触。一旦发现此类情况，就必须假定对方是便衣或线人。

我们保持镇定行走直至转入下个街角或脱离其视线范围，随即立即加速奔跑，通过反复切断视线接触直至彻底摆脱。

理想状态下，对方察觉到我们正在规避时，我们应该是已经成功脱身

了。

我们可能持续小跑离开该区域，选择自行车、汽车或无人机难以拦截的路线 —— 例如上下楼梯、穿过公园、商场、交通枢纽、人行天桥及隧道。掌握跑酷基础技巧的重要性再怎么强调都不为过，比如翻越围栏时避免脚踝扭伤，这需要练习。

[image]

详见相关自卫措施：[image]反监视

每次解散后，我们总要面临艰难抉择：是立即处理掉行动装备，还是先将物品转移到更远的地方（比如装进色彩鲜艳的提袋、购物袋或背包）再处理掉。我们权衡着离开这片区域时背包被搜查的可能性，据此来做出决定。即便袋中物品不足以在庭审中构成定罪证据，一旦被指控仍将可能导致数月乃至数年的压力与困扰。我们权衡着这种风险与另一种风险 —— 即警方取证小组可能在示威现场附近发现物品并送交法医实验室的结果。如果能安全将衣物和物资运出该区域，那就务必应该这样做。

当我们丢弃物品时，会有意识地选择警方取证小组不易发现的地点。我们力求将弃置物（已经尽力清除法医痕迹的物品）与衣物（必然残留部分DNA的物品）分开处理，让它们即便被发现也难以建立关联。如果需要弃置物品，我们会在行动分组解散前寻找隐蔽时机进行处理，确保解散后被捕者身上仅剩衣物。

离开现场时携带物品，如果您的衣着跟周围其他人没什么差别，那么被拦下特定搜查的可能性就会减少。待远离现场后，我们便会谨慎处理所有物品。

一周后的某个时候，我们将举行户外的集体会议以总结行动中的问题，全程所有人禁用手机。我们需要总结分析哪些战术奏效了？未来应避免哪些做法？哪些想做却未能实现？还有哪些问题需要厘清？是否需要设立被捕者支援机制？大家情绪如何？是否应（安全且匿名地）发布对事件的反思？下一步行动是什么？……

应对偏执的最佳良方是现实主义和充分的准备

在广泛社会抗争爆发之间的平静期，镇压力量只需应对相对少数的对手。我们采取本文讨论的所有应对措施，正是为了确保即使镇压力量投入大量警力资源打击我们参与的网络，我们仍能长期持续开展直接行动。

话虽如此，必须谨记近年来针对示威者的绝大多数案件仅依赖于少数几种易于应对的证据来源：

1、没戴面罩 —— 难免会遇到没戴面罩就往前冲的人。我们应该预见这种情况，携带几个装有黑色T恤和手套的包包，以便在现场分发给人们。一个简单的准备工作就可能改变人们的命运。

2、衣服上有标志或者特征明显，被识别了 —— 通过现场照片、监视视频录像、警方证词以及网购记录，任何具有辨识度的衣服都能帮助锁定“嫌疑人”。

3、没能遵守数字安全最佳实践 —— 例如发送了可被用于指控的短信，或因截图、照片、搜索记录、社交媒体使用情况或者手机定位记录而导致的后果。

4、没有遵循匿名购买原则 —— 如果购买敏感物资的时间距离示威活动的时间太近，商店监控录像对警方来说仍然比较容易获取，这些购买行为就更容易与身份建立关联。数字支付就更糟糕了，全部实名认证了。并且一些商品上保留的序列号或RFID标签也是同样的危险。

5、警方突袭住所搜查中被找到了“可疑物品” —— 正因此，我们必须处理掉所有可能与特定行为产生关联的物品，并将敏感物品存放在隐匿点或安全屋中。

关于"安全"的讨论往往导致人们不必要地自我设限。我们不想这样。相反，我们希望以一种能赋予我们实现抱负、发展更强大抵抗连续性的方式来探讨这个议题。虽然相互扶持永远伴随着风险，但我们可以努力不让敌人得逞。

[image]
[image]

街头搏击基本技巧（转帖）

[image] 关键词	个人 搏击 自卫
[image] 关联	；[image]武器和自我防御的重要策略：反侦基础课 S06E08
[image] 创建时间	2025年2月9日
[image] **Description**	行动安全性

街头是一个“不讲武德”的地方。您唯一的任务就是，活下来。

目前在国内练格斗的华人似乎没什么街头政治对抗的经验。在国外生活过的人应该有一些至少是旁观角度的经验，尤其是本世纪以来法西斯猖獗，政治性街头搏击基本已经自成一体，尽管专门的培训项目不太常见。

不论如何，有一些小经验，每个有可能面对风险状况的人都值得关注。

简单总结下：

1、

作为商业项目最常见的所谓综合格斗训练，其实在街头对抗的背景下意义不大。至少没必要专注于擒抱训练。即便练好了也只能应聘个保镖啥的，而且还要祈祷别遇到啥大状况。

所有地面技都如此，什么巴西柔术摔跤啥的，都基本是赚钱的生意，不是傍身的本事。

站稳才是防卫的根本 。

如果你跟一群人打架，你跟其中一个对手一起倒地的话，立刻就会有人踢你的脑袋或者背后捅你一刀，一切会在一秒钟内发生。

如果你想活下去，那就要让自己在任何情况下都不要倒地。

2、

避免那些具有千年高贵传统的花哨技术，不管是日本的还是中国，除非你只是为了传承艺术跟大佬合个影啥的。

这些东西都是为封建时代的职业种姓发展起来的，需要多年的全日制学习才能掌握并且基本涉及不切实际的过时的武器。除非你是地主士绅有能力做个武士。否则，关刀武士刀这类东西跟火车模型收藏没啥区别，都是玩物。

想在街上活下来，玩物派不上用场。

3、

如果你从来没接触过武术，感觉自己没有天赋，但很想要在遇到流氓时能自卫，那就练习一些最基本的东西。

比如踢腿，拳打脚踢，在徒手搏击的情况下必须的技能，泰拳对此有好处。

如果你预计会遭遇刀持有武器的对手，不管是钝器还是锋利武器，菲律宾武术会有帮助，比如Kali或Escrima。

如果你住在一个遍地是流氓并且每个流氓都有枪的地方，那你就只能给自己弄个好枪，去练打靶。

4、

不必专注于装备，包括武器。如果你会打，身边的一切都可以是武器，相反，如果你不会打，手持关公大刀也很可能挨揍。

即便你只准备徒手搏击，也要首先考虑指关节安全。

你不能戴着搏击手套到处走对吧。但如果你第一拳都把手指打断了，那就没有然后了。

所以手部的安全是要点。

5、

不必花太多时间研究缴械技术。

实战中最可能的情况是，你根本没机会用上缴械技术。

缴械尝试总是极其危险的。除非你的对手明显喝醉了，或者完全没有经验，并且周围还没有其他对手时，你才应该尝试缴械。

否则，你不应该试图解除对方的武装，相反，你应该尽可能使用你自己的武器。如果你没有自己的武器，又没有办法逃脱……那就真的有麻烦了。

6、

自卫大师经常说："首先，你应该尝试逃跑"。通常情况下的确如此，但并非总是如此。

首先，抓住对方总是比逃跑更容易，所以，除非你相信自己肯定能跑得比对手更快、并且准确地知道逃生路线的情况下，逃跑才有意义。

其次，你可能不是唯一一个生命和健康受到威胁的人，如果你能逃脱，但意味着抛下同伴，你还会跑吗？

显然，保持良好的体形并进行有氧训练总是有利的。几乎所有的街头对抗都需要耐力和至少一点短跑的技能。但你始终应该为无法逃跑的情况做好充分的准备。

7、

跟专业人士一起训练是有必要的。尽管的确很多这方面的专业人士都在捞钱、俱乐部乌烟瘴气、培训师麻木不仁，都挺普遍的，但还是要有专业教练才行。

只是不要被动听从教练安排所有东西，他跟你的优先事项很可能不一致，你要以自己的战略为指导，为了自己的需求，去请教专业人士。

你的目的是为了应对严肃的对抗，那就需要请求至少一个陪练人员，一个或者多个，多人的场景更真实。如果你的教练不了解陪练的重要性，那就换个教练。

[image]
[image]

S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

[image] 关键词	反监视 枪击 生存训练 社交工程 自主 自卫 街头 进攻 隐姓埋名 预防性
[image] 关联	[image]反监视 ；[image]反攻 ；[image]隐姓埋名
[image] 创建时间	2025年2月10日
[image] Description	行动安全性

[image]

要善良，同时要有足够的能力反击恶人。

能力，让我们的善良不至于变成弱点；善良，让我们的能力不至于沦为恶人。

[image]

这里特指现实中的反侦察技巧。行动者在现实中与政府间谍过招的技巧，以及应对灾难和突发状况的策略及工具。防备各种恶意的侵扰和威胁，包括绑架、抢劫等等。

您应该会在3种情况下用得到这些技巧：

1. 您不想让对手过早的知道您和谁关系密切，以避免被连锅端。

1. 行动后对手正在追踪您和队友，你们需要躲避追捕。

1. 气候灾难和环境灾害的日常防备。

[image]

S06系列服务于：敏感行动参与者；激进派前线行动者；直接行动活动家。

本系列提及的所有技巧和方法，仅在您真的明白自己在做什么的情况下，再尝试和练习。

列表

[image] 抢先采取行动 - 反侦基础课 S06E01：七点规则和态势感知

[image] 准确的情报和判断 - 反侦基础课 S06E02: 确立基准线

[image] 您必备的基本防身装备：反侦基础课 S06E03

[image] 如何摆脱手铐、绳索、束线带和布基胶带：反侦基础课 S06E04

[image] 如何撬锁、翻栅栏、短路点火发动汽车：反侦基础课 S06E05

[image] 特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06

[image] 警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 **S06E06A**

[image] 用“眼”识人 **-** 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 **S06E06A**

[image] 在你的日常生活中应用隐蔽野战技术 **-** 简单方法抵御敌对监视: 反侦基础课 **S06E06C**

[image] 如何欺骗，和如何防骗：反侦基础课 **S06E07**

[image] 武器和自我防御的重要策略：反侦基础课 **S06E08**

[image] 如何在大规模枪击案中幸存：反侦基础课 **S06E09**

[image]
[image]

抢先采取行动 - 反侦基础课 S06E01：七点规则和态势感知

[image] 关键词	反侦察 威胁响应 态势监测
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月11日
[image] **Description**	行动安全性

是的，需要练习，需要练习。只有熟能生巧。仅仅熟悉原理并不会带来保护。真正能保护我们的是条件反射式的专业级威胁响应。

- Table of Contents

规则1#：应变能力的训练
规则2#：自救
规则3#：自知，而不是自满
规则4#：行动起来以拯救生命
规则5#：洞察力决定一切
问自己这些问题：
规则6#：注意基准线
规则7#：不论任何时候都要保持态势感知
反侦查行动力的基本功
白色态势 ——
黄色态势 ——
橙色态势 ——
红色态势 ——
保持黄色态势以避免红色态势

[image]

生存的基础是危机响应。良好的危机响应需要出色的应变力。

要做到这点，您需要遵循几条重要的规则。

规则1#：应变能力的训练

生活中几乎没有恰到好处的完美。保持对环境动态的敏锐捕捉、和持续满格的应变能力，是生存的必需。

懂得在紧急情况下该做些什么固然重要，但能挽救您的依旧是应变能力。就如 Hakin9 的训练 ，它注重于测试您的实战技能，而不是单纯记住书本上的知识。

生活很难按计划进行，而智慧就是，随时都能充分利用现有的一切去解决迎面而来的难题。这一点至关重要。

您会发现，虽然反应灵敏、身体强健、力量强劲等等都很重要，但是，如果无法对潜在的新威胁随机应变，这些辅助条件的作用最终都是局限的。

规则2#：自救

您首先应该相信的事就是自救，而不是等待他人来保护您和您的亲人的安全。这超出个人哲学的范畴，它是本系列的主旨 —— 因为我们必须首先有足够多的人擅长自救，才能有实现互助的基础。

现实中往往存在一些最初远不至于如此，而最终由于自救能力缺乏而导致惨剧的实例。

从意识层面依赖自己，而非他人，这是最简单的最靠谱的途径。

只有在您足够强大的时候，您才可以帮助更多人。

规则3#：自知，而不是自满

您应该能够准确评估自己的能力和现实中手边可取的条件，高估或低估都是有害的。

这说起来容易，但实际上并不容易做到这点。您肯定知道达克效应，越是能力不足的人，越容易轻敌并高估自己。

您在互联网上经常能见到那些夸夸其谈的人，看起来就像他们能力很强一样，其实完全不然；真正技能高超的人都是沉默寡言的，因为他们能看得很深，于是更理解什么叫山外有山。

您不需要追求成为无敌的终结者，只需要对自己的实际能力有一个相对准确的评估，对环境有一个更加充分的认识。

保持信心，但必须灵活运用。

[image]

规则4#：行动起来以拯救生命

灾难都是突如其来的，而幸存者是那些没有被突如其来吓呆以至于失去行动力的人。

行动起来，是拯救生命的关键。虽然这也并不容易。人们真的会因惊愕而呆滞，原本学到的东西瞬间似乎被清空了一样。这非常可怕。

想象一个人拿着刀子，朝你扑过来，这种情况下赤手空拳的你只有两种选择 —— 逃离，或被刺伤。如果你被吓呆了，那结果只能是见血。

显然这是简化的解释。但要知道，它的适用范围非常广泛。当威胁到来时，动起来是求生的第一要务。在坠机中幸存的人都是那些能够及时离开座位并行动起来的人。

规则5#：洞察力决定一切

本系列中的内容基本简单易行，您可以在扔下手机后几分钟内实践它们。

这是因为洞察力很重要。

您可以了解到在多种情况下需要采取的行动、如何给他人留下对您有利的印象。这是身体和心理两方面结合的技巧。

您真的知道自己留给他人的印象是什么吗？准确评估这点非常重要 —— 这样您才能准确调试这一印象，以令其符合您在不同场合状态下的切身利益。

问自己这些问题：

- 我看上去像受害者吗？
- 我的家看上去像没入居住的地方吗？
- 我走路和说话时的姿态是看起来信心满满还是弱不禁风？
- 周围人都是什么情况？

- 餐厅里坐在我后手方（盲区）的那个人是否可疑？
- 刚才路过杂货店时是否被尾随了？
- ……

学会保持警觉是致胜的关键。这也是反侦察行动的基础。

规则6#：注意基准线

准线就是所谓的常态，这是情报界的重要理念之一。

除非您非常熟悉某个特定场所的常态 —— 也就是说，那里是您的地盘 —— 否则，您必须知道 “客场” 作战不应该采取哪些方式 。

想必大家都看过很多游击队的故事，游击战中行动者先将对方引入自己的地盘，然后往死里折腾他们。这就是基准线技巧。

那么哪些是您的地盘呢？您的家、您生活的社区、您工作的街区 ……等等，都应该是，也就是说，前提是，您必须对自己生活工作的区域保持一种强大的了解和熟悉。这就是观察和记忆的能力 —— 情报和反情报基本功。

规则7#：不论任何时候都要保持态势感知

这是最后一条规则，也是一个基石。简单说就如中国俗语，“先下手者为强”，您和您的对手，谁能先下手，谁就能抢得主导权。要做到

这点，您就必须对周边的态势保持准确的感知力。

其底线在于，如果您对周边的细微变化不敏感，那么本系列中传授的所有技能都将落空。

如果您低头玩手机、对美女目不转睛、专注于与朋友闲侃 …… 所有策略都不会生效。攻击者经常会采取社交工程手段，先转移你的注意力到诸如美女等闲杂无关的东西上，然后在您的盲区里制造致命袭击。

态势感知和受破坏妄想是截然不同的两码事，千万不要混淆它们。态势感知需要您准确了解周边真正发生的东西，而不是靠想象力，您需要尽可能将盲区降至最低，并随时准备好排除那些想要误导您的烟雾。

态势感知能帮您在遭受袭击之前采取行动制止威胁。这需要练习，还需要保持专注。但请相信这是可以做到的，而且是挽救性命的关键。

于是接下来我们将首先介绍这一基石：态势感知。

[image]

反侦查行动力的基本功

任何一种包含对峙技巧的训练中，第一步要学习的就是态势感知。此后才是如何躲避各种袭击、如何逃脱束缚、如何追逐 …… 等等。

抢在危机发生之前采取行动，就是态势感知能帮您做到的。如果已经到了不得不拔枪的地步，那只能说明态势感知能力缺乏。

一般人作出反应所需的时间大约是 1.5秒 ，这很慢，经过训练的人肯定要做得更快。

如果您不能保持警觉和清醒，就很容易遭到攻击。

如果您曾观察过街头、运动场或商场里大部分人的行为，就会发现一个共同点—— 绝大多数人不是在用手机聊天，就是在发送和阅读文本信息。如果是在玩手机，就会低下头，对周围的环境没有觉察，就会对身边正发生的事情茫然无知；或者也可能您没有用手机聊天，却为工作所困，压力重重；或者只是在幻想接下来的假期该怎样度过（走神儿）。

在很多情况下，如果人们能发挥态势感知能力，许多伤害实际上都是可以避免的。

手机只是一个太过普遍的现象，但您必须知道， 诱导以牵制您的注意力的东西远非只有手机。

陆军中校杰夫·库珀70年代时在亚利桑那州创办了全国手枪协会，教授平民如何使用来复枪自卫。库珀虽然在枪支火器方面闻名，但他也同时相信， 最有效的武器其实是人的思维模式 。

库珀用颜色代码来描述不同等级的态势感知力，具体如下：

白色态势 ——

毫无防备，完全无意识。那些专心玩手机、瞟美女、围观看热闹、走神儿的人都属于这种。关键在于，您需要努力避免这种情况。

表现 ：低头、眼神飘忽，对周围发生的事心不在焉。

坐在公园长椅上读书、夜晚不假思索地走入一条黑暗的小巷，很容易将自己置于易受攻击的境地。

如果您对周围环境中发生的事不加留意，您就会处于弱势，不管接下来发生什么，您都会毫无防备。

黄色态势 ——

处于黄色态势意味着没有特别的威胁。或许您正在和某人交谈，但不会分心到看不见迎面而来的卡车或人的地步。

处于黄色态势的人在街上一定会注意到正靠近自己的奇怪的人，而且有足够的时间决定如何行动。

黄色态势让您能意识到是否会碰到麻烦。记住这点很重要， 保持黄色态势能让您远离红色态势 —— 那种你肯定不愿意发生的事 。

表现 ：昂头，对周围保持警觉。

橙色态势 ——

这是进一步保持警觉的状态。

比如，已经是6月初的天气，却有一个人穿着厚重的外套在一座人潮拥挤的大厦前闲逛；或者您在去停车场的途中感觉到有陌生人对您的关注度过了头 ……

简单说，某种环境或某个人让您意识到存在潜在威胁。这种情况下您的手已经伸进口袋，握住战术防身笔或枪，也许是准备好了拨打电话以求救。

表现 ：橙色态势意味着您已经需要开始准备反攻了。

红色态势 ——

红色就是处于危急的形势，但您已经做好了迎战准备，预先判断是清

楚的。

现在开始进攻。发生搏斗的可能性非常大，您需要调用一切您拥有的武器或防御策略。

表现 ：行动力。也就是不要被吓住，而是要以最快速度作出反应。处于红色态势的人可能已经找到逃生处，而且正在飞奔；或者开始搏斗。

保持黄色态势以避免红色态势

如果您正在执行敏感的任务，一位漂亮女士举着香烟走过来借火，这时候您需要关注的不是打火机放在哪了，也不是漂亮女士的身材，而是周围是否还有其他动静， 尤其是您的盲区 —— 背后 。

如果有人从后面袭击给您套上黑头套，那位女士就只是帮凶。

这只是一个比喻。保持黄色态势的警觉就是要这样，这是一个逐渐适应的过程，但小的改变就足以让您在正确的道路上迈出一大步。比如，不要看手机，昂首走路，随时对四周有所察觉。

倾听也是非常重要的，如果危险降临，还有另外一些策略能帮您变得更加敏感。

[image]
[image]

准确的情报和判断 - 反侦基础课 S06E02: 确立基准线

[image] 关键词	反监视 基准线
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月12日
[image] Description	行动安全性

您的观察和记忆的能力对于反侦察来说至关重要。

- Table of Contents

  预发信号1#：盯视
  预发信号2#：步速
  预发信号3#：注意力干扰
  打破正常化偏见
  建立基准线的秘诀
  那么，究竟何为基准线
  从人类标准行为开始

[image]

不管是镇压武器还是政府间谍，所有威胁都仅在您毫无防备措手不及的情况下最为有效。措手不及是一种个人层面的情报失误。

很多受害人曾表示，他们完全不知道会遭遇袭击。但事实上，绝大多数袭击者在行动之前都会暴露一些信号；或多或少，以各种形式体现，包括比如眼神接触、跟随您的步速等等，只要您能保持黄色态势

的警觉习惯，就不会容易遇到剑拔弩张的红色态势局面。

预发信号可用来描述一个人在特定形势下将会采取的可预见的行为模式。

您必须了解一些可辨认的的预发信号，以便及时作出反应。

预发信号1#：盯视

在将您锁定为攻击目标之后，攻击者会盯住您一段时间，这是为了寻找最恰当的时机。这个时间长度足够令人感觉不适。

如果您注意到有人盯着您的时间过长，就应该提醒警惕了。可以迅速穿越街道寻求帮助，或者快速采取反追踪策略，不惜一切代价以逃离对方的视野。

您无需担心误判，因为真正的攻击者会下定决心追踪您，就像捕食者用目光锁定猎物那样。

预发信号2#：步速

所有人都在街上走，采取的都是自己舒适的步速；而只有那些心怀不良意图的人才会跟随您的步速。

与陌生人保持同样的步速对人类而言是很不自然的，于是这是一个很容易捕捉到的信号 —— 您会意识到自己正在被跟踪。

请注意：这一点对汽车来说也同样适用。

如果在公路上您发现您的车子和别的车子并排行驶，其中一辆车就必定会加速或减速。

如果您改变自己的车速就会发现，追踪者也会改变车速以试图与您保持一致。这就是一个明显的信号，意味着您应该迅速想办法逃离以保证安全。

尤其是，如果您是敏感人士，并且正在参与一项保密的行动，途中您发现尾随车辆的存在，请注意：您的对手很可能不止一个，当您成功甩掉其中一辆车子时，在下一个路口可能出现另一辆车子跟上你；您需要快速记住尾随车辆的特征/车牌，以便通知队友，以及在接下来的行动者锁定对手。

预发信号3#：注意力干扰

还记得上一集中漂亮女士借火点烟的案例吗？—— 诱导目标分心是攻击者的最常用手段；这一手段会表现为很多种形式，比如一位看起来可怜的老妇人急匆匆地请求你的帮助、甚至一个普通的小孩子走过来和你说话，等等 …… 这种情况下您的注意力首先不能放在美女、老妇人和小孩子身上，而是您的盲区—— 您的背后及两侧。

[image]

大多数攻击者都是团队行动的，尤其是政府间谍，其中一个人专门负责诱导，目的是锁定你的注意力在无关紧要的东西上，并因此拉低你的态势警觉度。

[image]

打破正常化偏见

“正常化偏见” 就是人类处理意外变化时的表现 —— 它是一种下意识的应付令人不快的事件和灾难的方法。心理应激反应。

人类天生就害怕变数。每当有大事即将发生或正在发生时，例如，灾难性流行病的爆发、飓风、恐袭等等，人们会下意识地在心里竭尽全力将事态 “正常化”。就如911幸存者所言：“给我一百万年我也不可能想到会遭受这样的袭击，它完全不在我的考虑范围内，我的大脑无法应付这个” ……

正是这种正常化偏见强迫人们以为 “一切都会没事”，即将到来的灾难 “可以控制”。这就会将自己置于危险的境地。

正常化偏见是人类大脑的一种自我保护机制，但是，我们必须学会抵抗这种偏见，因为它非常危险。

每一种有效的行动都需要事先充分的情报、和完善的情报分析，情报的目的就是给您时间打破正常化偏见，以作出先验的风险计算。

如果对某个事件可能造成的影响没有清醒的认识，您就不可能做出有效的应对准备。如果放任不管，正常化偏见就会导致人们做出危险的行为。

人类习惯的思考方式有很多缺陷，最明显的比如，认为某件事从未发生过，那么它就 “永远不会发生”。这样的想法在碰到新情况时就难以做出反应。

这并不是说您必须在任何时候都保持忧心忡忡，绝对不是，而是说您需要认识到有这么一种东西它叫正常化偏见，随时都在误导您的决策—— 您需要学会控制的心态，这样才能发挥敏锐的态势感知力。

建立基准线的秘诀

那么，如何判断一个看似正常的环境是否会变得危险呢？

如何搜集细微线索才能明白某事即将发生—— 情况并不像表面看起

来那样？

这就是基准线能帮您做到的。

建立有效的基准线需要您注意某个具体场所或某个人行为上的重大或细微的变化。

也就是说，您首先需要对其他人和所处环境的情报进行快速和准确的收集。

福尔摩斯的故事尽人皆知，其中充分体现了基准线的原理。

比如，夏洛克初识华生时他随意问到："伊拉克还是阿富汗？" 根据华生的回答（阿富汗）以及同他共处的几秒钟时间。夏洛克就可以判断出，华生是一个受过伤的军医，他是来看理疗师的。而且理疗师认为华生的跛足是源于身心失调。

华生自然对夏洛克的精准判断目瞪口呆，当他问起夏洛克是如何知道的时候，夏洛克回答："我事先不知道，我是靠观察发现的"。

这就是基准线的秘诀。

夏洛克解释说："你的发型、你对自己的严格要求。说明你出身军队；进门后你说过曾在巴茨受训，因此是军医。你的脸是棕褐色的，但是与手腕以上的肤色不一致—— 你一定出过国，但不是为了晒日光浴。走路时跛足很严重，但站立时并没有倚着椅子，好像你已经忘了自己的脚，所以至少有部分原因是身心失调。这就意味着，你当时受的可能是外伤—— 那么就是在行动中受伤的。在行动中受伤，脸棕褐色—— 阿富汗或伊拉克。"

[image]

那么，究竟何为基准线

您可以保持黄色态势，警惕周围的环境，观察哪些正常哪些不正常；但是，如果您的大脑无法让你看清楚或者记忆准确，并做出反应，那么您就不可能采取适当的行动保证安全。

要判断情况是否正常—— 无论是针对个人还是某个地方，您都需要设置一个基准线。

基准线指的是一种非正式的的衡量标准，用以判断形势正常与否。

比如，当一个好友告诉您：“你最近看起来满面红光啊”，这就是一种衡量比较，因为他知道您 “平时” 什么样，也就是说日常标准—— 这就是他了解您的基准线。

他能够注意到，您是不是晒过太阳、是不是休息得很好、是否心事重重，等等。

看到没，这一点都不难。如果孩子平时胃口特别好，而今天忽然说不饿，那么作为父母，您肯定知道出问题了。要么孩子身体不舒服，要么是零食吃太多了。当然对于其他小孩子来说这也许很正常。

这个比喻也许会产生一些误解，也许您会觉得 “我肯定知道我的孩子和我的哥们的基准线”，是啊，因为您对他们很熟悉；但是，在防御灾难的用例上，您的熟悉范围必须更大，而且要具备高人一等的记忆力。

简单说就是，您需要能准确判断您所处的环境中哪些属于正常、哪些属于不正常。我们在反侦查的内容中也强调过这点。

环境也有基准线。

就是那些摄像头的用例之一。

比如一栋银行大楼。摄像头传感器摄取信息时能够判断何为警戒线的

正常状态；如果超出正常范围的事发生，运营中心就会收到通知。

这不是完美的，而且需要不断调整标准，但是原理是一样的。举个例子，几个背着大型双肩背包的人走入酒店大堂的餐厅。大型双肩背包是日常范围的危险信号 —— 可能需要怀疑里面有武器、炸弹之类的危险品；但是，如果您知道一支游泳队正下榻该酒店，并且他们在准备参加比赛，这种背包可能就不足为奇了。

换句话说，如果整个大厅里只有一个人背着这种背包，并且没有例如游泳队这类背景信息，那么您应该提醒警惕。

当然，袭击者也很聪明，他们会实现勘查环境情报，并选择例如游泳队出场的背景，以化妆成队员的一部分，混入攻击地点。

但他们的神色会暴露他们与众不同。这需要您及时捕捉和甄别。

[image]

如果有人动过您的桌子，您能及时发现吗，即便对方没有拿走任何东西？如果你居住的街道存在潜在威胁，您能辨别得出吗？如果你的队友忽然 “表现奇怪”，您如何判断他是否已经背叛你们的组织？……

要做到这一切最基本的就是：您的强大的观察和记忆的能力。

从人类标准行为开始

显然大多数人不可能追求夏洛特那种推理能力，但是您肯定可以从中学到东西，从而帮助您在日常中更准确地识别人和事物。

尤其是，懂得如何在微笑细节上了解一个人和一件事，至关重要。

我们所受的教育让我们努力去欣赏彼此的差异，我们被告知，接受他人不同的行为是一种礼仪。但是，您应该知道，正常、非同寻常、不

能接受，对于他人的行为来说有可能是上述任何一种情况；它还会受到诸如文化、价值观、和态度等其他因素的影响。汝之蜜糖彼之砒霜。您需要全方位地考虑才能做出准确的判断。

比如，在法律事务所的人穿西装打领带肯定被认为是非常得体的，但如果一名建筑工人穿这一身露面，也许就显得怪异了。观看体育比赛时大呼小叫是正常的，但看话剧时这么做就显得很没规矩 ……

人类的标准行为会根据不同场所而发生变化，根据直觉，如果有人的行为异常，您就需要谨慎行事。

以下几点可以作为参考标准，也许不够完整，但基本面是足够的：

1、这个人的衣着符合当前的天气状况吗？明明已经很暖和了却还穿着厚重的冬季外套？

2、这个人做出了奇怪的手势和举止吗？

3、这个人出现在了他不应该出现的地方吗？

4、这个人是否对你和其他人的关注过于密切？

5、这个人看起来是不是像在跟踪某个人？

6、这个人打量四周的时候是否看起来有点紧张？换句话说，他的脑袋是不是不停地转向四方？

以上这些说起来并不难，但要真正做到—— 也就是令其有效—— 却不那么容易。这需要日常的训练，有意地培养自己这种观察和觉察的能力，记忆的能力，分析判断的能力。

您永远都无法预知何时何地会面临生死攸关的境况。

如果没有食物和水，且得不到外界救援的情况下，您和您的家人能幸存吗？当您驾车外出时，如果遭遇严重危机，您能坚持多久？如果参与敏感聚会途中被绑架，您可以如何脱身？……

人们经常不会去考虑这些问题，这就是为什么普普通通的攻击模式也能屡屡得手。

希望S06系列内容能给您一些帮助。

本系列前两集讲述的都是心理层面的防御，这是一个最基本的层面，接下来我们将讲述现实行动力层面的防御方法。从装备开始。

[image]
[image]

您必备的基本防身装备：反侦基础课 S06E03

[image] 关键词	工具 自卫 逃亡 预防性
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月13日
[image] Description	行动安全性

关于您应该准备什么的清单。

- Table of Contents

三个等级救生装备 —— 特工人员的随身工具包
一级：日常装备
1、折叠小刀
2、手机
3、发卡
4、猴拳结伞绳钥匙链
5、手铐钥匙
6、钱（现金）
7、战术防身笔
8、开锁工具
9、信用卡刀
二级：手提电脑包装备或手提包装备
1、防弹板
2、开锁工具包
3、雨披
4、止血剂
5、手电筒

6、多功能工具钳
7、汽车钥匙
8、布基胶带
9、火源
10、伞绳
11、录音笔
三级：汽车装备
1、斧头
2、拖缆
3、手动曲柄收音机
4、打火机
5、撬棍
6、急救箱
7、当地地图
8、小刀
9、折叠铲
10、72小时工具包
人工情报
1、安全通道和死角
2、医院
3、药店
4、水源
5、当地的市立机场
6、食物和水：准备自己的供给
立即行动起来

[image]

知识是最重要的基础工具。在有些情况下，一些少量的补给和少量的工具就能拯救您的生命。因为您具备足够的知识，您知道该如何运动手边的一切资源。

您不需要成为专家，单一领域的专家反而会局限人的能力。但您必须熟练，必须有经验和耐力，这需要以心理层面的“工具”为基础，也就是本系列前面的内容所强调的 —— 准确说是训练。它是日常工作的一部分。

本集内容提供的工具列表既适合日常安防配备，也适合逃亡途中伴身。

[image]

本集内容对应“自卫措施”：[image]隐姓埋名

三个等级救生装备 —— 特工人员的随身工具包

如果问人们情报人员会携带什么东西以防身，大多数人总是会首先想到那些了不得的东西。但邦德式的装备只是电影而已，事实上真正的间谍只需携带一些看起来很普通的小物件，就能达到目的。

这些小物件方便携带，而且价格低廉，最重要的是，您需要会使用它们。

这里将这些装备分为三个级别，以方便您识别哪些最适合自己。

一级：日常装备

日常装备就是随身携带的放在口袋里的东西。

1、折叠小刀

一般可以放在前裤袋里，这样可以方便拿取。在购买的时候您可以试试是不是顺手。

一把放进口袋的折叠刀就可以是防身和逃生的必备物品，希望您最终不至于用它来搏斗。

2、手机

这是为您方便与亲密队友保持联系。我们不支持使用智能手机，智能手机本身是贴身间谍，它会泄漏您的身份信息；并且在很大程度上它会影响您的态势感知力。

这里讲的手机就是用来打电话的，没有其他用途。您需要在危难的时候有顺手的求救渠道。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

3、发卡

这东西听起来可能有些奇怪，后面的内容将具体说明这点，关于为什么一个便宜的发卡也许就能帮您摆脱危机。

4、猴拳结伞绳钥匙链

伞绳（就是550绳或降落伞绳）有很多惊人的用途。它结实的程度可以令人难以置信，能帮您摆脱一些严重的危机。同样，后面会具体介绍。

猴拳结本身也是很出色的自卫工具，因为绕着这个滚珠打成的伞绳结如果用来对人发起攻击，会造成严重的伤害。

5、手铐钥匙

这个东西能带上飞机，所以无需担心被安检没收。

6、钱（现金）

现金真的很管用。有些时候只有它就能帮您解围。

不只是用来买东西的，而是，有些时候您需要帮助，塞给对方一些钞票，就很容易获得协助。您永远不知道什么时候需要向他人小施恩惠。

7、战术防身笔

它是非常出色的防身工具，可以适用于每一个人。

乍看起来它就像一支普通的钢笔，可以用来写字。但同时它也可以用来阻止袭击者。

战术防身笔采用航空级铝合金制造，笔尖坚硬有力。如果遭遇事故，或者需要在车子落水之前逃出去，这支笔的笔尖既可以用来阻止袭击者，也能够戳破车窗玻璃。

如果您遭遇袭击，使用这支笔瞄准对手的眼睛、肾脏或者腹股沟，就可以趁机逃生。那种疼痛是非常剧烈的。

具体使用方法后面将做详细说明。

战术防身笔几乎可以被带到任何地方，不论是上飞机还是出入重要安全设施。

8、开锁工具

这也是必需的，因为您有可能遇到需要从上锁的房间里逃出去的时候。或者打开任何房门，或者您自己和邻居被所在屋外了，这个东西也非常管用。

一般情况下开锁工具也能轻松通过安检。但是携带之前您需要了解一点法律，因为在不同地区有不同的管制规定。

9、信用卡刀

对于那些不习惯在衣服里别一把刀具的人来说，信用卡刀可以是个好主意。尤其女士，相比常规的刀具，更合适使用信用卡刀。

信用卡刀是一种非常精巧的工具，它可以折叠成信用卡的形状，以确保安全和方便携带。刀锋从卡的中间位置弹出，然后向两边折叠，扣紧到位。这个原本只是放在钱包里的“信用卡”瞬间就能变成一把锋利的刀，可用来自卫和逃生。

[image]

二级：手提电脑包装备或手提包装备

1、防弹板

最好是3A级的那种，采用的是制作警用防弹背心的材质。如果你遇到了持有钝器的袭击者，这种防弹版可以帮您提供最高级别的保护。

[image]

返回：[image]了解防弹衣：街头实战指南 S05E08

2、开锁工具包

显然您需要查看一下法律规定。一个全尺寸的开锁工具包能帮助您在很多情况下获得逃生的机会。

3、雨披

不言而喻它用来挡雨，但是也可以用于紧急避难，比如遇到车祸、地震、塌陷等等状况时。

4、止血剂

止血剂就是纱布，只不过上面带有能加速凝血的药物。如果您不小心被伤到了，止血剂能帮您解决问题，还能防止感染。

5、手电筒

大多数时候手电筒都会很有用，建议选择小尺寸的迷你手电筒，在下面看到视频。

https://youtu.be/bhbhtodwpCc

6、多功能工具钳

这种工具钳可以把老虎钳、刀、螺丝刀和其他一些工具集于一身，可以在很多状况下派上用场。

7、汽车钥匙

记得自动售货机用的那种金属片钥匙吗？差不多就是那样，基本是一个汽车开锁工具。锁匠、汽车销售商、拖车和回收公司都用它。

如果您碰到紧急情况，需要迅速逃离，不得不占用别人的汽车使用短路点火启动时，这种工具可以帮您进入老式汽车。

将它插入锁里轻轻晃动，就可以打开1999年以前的汽车。

8、布基胶带

基胶带的用途很广泛，也很适合随身携带。您可以用它来修补帐篷上的漏洞，或者把东西绑在一起做成临时庇护所。

布基胶带非常结实又耐用，网上有很多视频可以找到关于基胶带的有趣用途，比如制作钱包、甚至吊床等等。

9、火源

这个不是给您点烟用的。即便不吸烟的人，随身携带打火机也很重要。如果碰到需要生火取暖的情况，或者加工食物，有备无患肯定是好的。

10、伞绳

伞绳有很多惊人的用途，后面将逐步介绍。

11、录音笔

当然手机可以帮您录音，但智能手机本身不够可靠，于是录音笔会是个好主意。

如果遇到某个您无法信任的人却需要合作，那么最好录下整个过程。当然，首先也要了解一下您所在的地区的相关法律。

三级：汽车装备

1、斧头

小型的那种就可以，放在工具箱中，在需要劈柴和砍断拦路的树木时

会非常趁手。

2、拖缆

拖缆能帮助您将汽车从困境中拖拽出来。当您需要绳索捆绑东西，例如固定货物、搭建临时庇护所时，会非常实用。

3、手动曲柄收音机

在紧急情况下，不要指望依靠手机或汽车收音机，它们可能都无法使用。手动曲柄收音机能让您随时了解形势的变化，而且您无需担心电池问题。

4、打火机

是的您的公文包里已经有一个打火机了，现在在车子里再放一个，双保险。

5、撬棍

在砸破车窗或突破栅栏之时，撬棍会很管用。它还可以做杠杆和控制杆。

6、急救箱

简单的那种家用急救箱就可以，基本可以解决外伤问题，记得要配止血剂。

7、当地地图

如果您需要匆忙离开，必须了解地形，能迅速找到目的地和来回的路。紧急情况下不能指望手机和GPS。

8、小刀

基本型的求生刀放在车子里，双重保险。

9、折叠铲

折叠铲很适合放在车子里，在需要从雪地或淤泥中挖出轮胎的情况也不是不可能遇到的。

10、72小时工具包

如果您在不明地点遭遇事故，车子抛锚了。或者被困在雪地里，这个小背包中的物品足够您保命。

包中装有足够维持3天的食物和水。它体积很小，不会占用车子里太多空间，而且它很重要。

要预制这样的小包也并不难。您需要的是下面这些物品：

- 食物棒：只需要6条高能量食物棒，每条400卡路里，而且应该是防水包装。
- **6**盒过滤水（**Aqua Blox**）：这些水足够撑3天。这种水可以保值5年。
- 净水药片：至少需要准备10片净水药片。10片能净化5瓶两升装的水。使用时直接丢进水里就可以里，等待几分钟，水就可以安全饮用了。

- 双波段收音机：还要确保有电池。收音机可以让您在紧急情况下收听广播电台发布的状况指南和天气预报。

- **LED**手电筒：可充电的手电筒。那种挤压手柄就能充电的手电筒很不错。

- **30**小时求生蜡烛：这种蜡烛可以调节烛芯，而且还能用作野营炉加热食物。

- 五合一应急求生口哨：除了口哨外，五合一还包括反光镜、指南针、防水火柴盒、点火用的燧石。

- 防水火柴：一定需要是防水的，避免在紧急情况下被打湿。

- 应急睡袋：睡袋应该能很好的防风、防水、能保存你身体90%的热量。

- 应急雨披：需要准备带有帽兜的雨披，这样可以将整个身体保护起来。

- 求生刀具：包括16种不同的工具，例如十字头螺丝刀、开罐器、螺丝锥、钻孔器、修甲刀、坚固的铰刀、槽螺丝刀、钥匙圈、牙签、镊子、木锯、刀片和开瓶器等。

- 防尘口罩：需要是合格产品。

- 口袋装纸巾：至少3包。

- 防护眼镜：遇到灾难时保护眼睛不被杂物所伤。

- 针线包：用于修补衣服、帐篷或其他躲避处的裂口。一定要有安全别针、缝纫针、纽扣和线。

- **24**小时洗漱卫生工具：牙刷、牙膏、湿巾、小块香皂、洗发水、牙线、护手霜、除臭剂、剃须刀、梳子、毛巾、护垫……

- 小型急救箱：不同尺寸的创可贴、布条、消毒片和纱布。

- 便签和铅笔：紧急情况下写下重要信息。

请记得，并不说您需要马上行动以配备上述所有东西，您应该先考虑清楚，这三级救生装备中哪些物品最适合您。但至少，您随时可以着手准备救生装备了。

[image]

越早越好，因为您需要在安全的环境下多尝试这些工具的使用方法。

[image]

人工情报

人工情报（HUMINT）就是通过人工搜集到的情报；换句话说，就是在当地搜集信息的工作。

如果您抵达一个陌生的地方，要做的第一件事就是搜集情报：尽可能多地了解这个地区内的一切。

如果您就在自己的家乡，那就更应该如此。

您尤其需要记住以下内容：

1、安全通道和死角

如果您需要步行或开车逃离，该走哪条路？死角就是那些有可能发生拥堵的地方。

您必须对所在地区的环境足够了解，才能在危机发生的时候迅速找到出口。

如果您被恶意者（比如政府间谍）尾随了，想要甩掉他们的关键就在于您对路径的熟悉。

[image]

如果您参加一次敏感的聚会、会见一位敏感人士，您一定不希望被监视者觉察到；于是您需要尽可能兜圈子，用多个虚假的“目的地”淡化真正目的地的可见性。这也同样需要您对地形和对手的思考方式有充分的了解。

这一切都在于平日的积累。如果您下班回家的途中偶然看到一家新的商店出现在路边，最后却了解到这家店几个月前就开张了 …… 那样可是不及格的。

2、医院

距离最近的医院在哪里？哪条路可以最快速抵达那里？如果很难前往那里，还有哪些其他选择？这些选择中哪个应该最靠谱？

这些问题的答案都需要平日心中有数。

3、药店

您需要知道在哪里能买到药品，如果您和家人生病了，如何以最快的速度购买到药品，这很重要。

4、水源

如今绝大多数家庭都有自来水，拧开龙头随便用。但危机情况下可就不一定了。您需要知道，如果自来水停了，您可以在哪里取水维生？

5、当地的市立机场

尤其是当您抵达一个陌生的地方时，记住机场的位置、通道、航线等等是很重要的。

6、食物和水：准备自己的供给

平日擅长储存不仅能帮助您在突发的危难中维持生命力，而且也能保持足够的内心平静 —— 紧张焦虑会耽误您的求生技能的发挥。

显然不是所有人都有足够的经济基础或者储存空间，但您准备得越多，情况就能越好。

[image]

立即行动起来

不论您是参与敏感行动还是应对气候灾难，平日里的准备工作越充分，您就具备越高的快速行动能力。行动得越快，生存的概率就越高。

对于本集内容中列举的这些基本装备，您应该在危难发生时以最快速度将这些武器带在身上。

还请记得，如果有需要，几乎所有东西都能成为武器，包括石头、玻璃碎片、大棍子等等。

显然，能拿出72小时工具包是最好的。如果能拿到，那就去拿；如果

拿取它会导致您被置于更危险的境地，那就必须放弃。

您必须准备足够的应急现金。如今的人们都喜欢使用在线支付，然而一旦危机发生，切断了电力，您的手机无法打开、系统故障、银行被迫关闭，您熟悉的途径完全失效，您必须有现金作为后盾。

并且如您所知，现金相比下是最值得信赖的隐私安全媒介。

现金使用的越少，它作为后备力量的效果就越差。已经有很多报告警告过，即使是现在，如果数字或电力连接下降，所有正确的地方都没有足够的现金来保持经济的长期运作。

这很危险。如果您能确保在自己家中备有足够的现金，也许会很有用。

[image]
[image]

如何摆脱手铐、绳索、束线带和布基胶带：反侦基础课 S06E04

[image] 关键词	个人 威胁响应 逃亡
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月14日
[image] Description	行动安全性

用尽您能用的所有办法，不要放弃，不要慌乱，使用技巧而非蛮力。

- Table of Contents

如何摆脱布基胶带
步骤1:调整姿势
步骤2: 挣脱
故障排除
B 计划：如果您是从背后被胶带绑住了或者受伤了，怎么办
如果双手、双脚和嘴巴都被胶带缠住了，怎么办
如何摆脱束线带
步骤1: 调整姿势
步骤2: 旋转锁扣
步骤3: 挣脱
故障排除
B计划：伞绳方案
如何摆脱绳索
步骤1: 调整姿势
步骤2: 前伸和摇动

B 计划：用伞绳摆脱绳索
如何摆脱手铐
方法1: 弯曲的发卡
步骤1 ：工具
步骤2: 摆脱手铐
故障排除
方法2: 条状发卡制作的垫片
步骤1: 工具
步骤2: 插入垫片
关于后备厢的挑战
当被黑头套绑架 …… 现在该怎么办

[image]

大多数人家里都有布基胶带，那是用来打包纸箱的，或者修补一些东西。但是布基胶带在绑架或入室抢劫的情况下，就是被用来制伏您的东西。

一旦被绑住了手腕，大多数人会放弃挣扎，从精神上就妥协了，因为他们不懂得该如何逃生。

其实有一种方法可以帮您在几秒钟内解脱。

了解逃生的办法可以帮助您临危不乱，更加有力量和信心。下面我们分头说，从最简单的开始。

如何摆脱布基胶带

这种胶带是最便捷最简易的绑束工具，于是您基本可以肯定在被绑架的情况下，遇到这种东西的可能性会非常大。

不要慌。慌乱不仅不能帮助解决问题，还会导致您学习过的技巧一时想不起来，那就糟了。

无疑，被绑住后会令人感觉心力交瘁，尤其是，即便您很有力气、有着粗壮的臂膀，也是扯不断它的，单纯地扯动不起作用。

[image]

因为，摆脱胶带的关键不在于力气，而是要懂得如何创造新的角度，以便容易让它扯破。如果您曾经撕断过一片胶带，那么您就会知道，只要找到正确的角度即可。那就是您现在要做的事。

步骤1:调整姿势

尽可能将身体前倾，手肘和小臂紧靠在一起。如果能做到，那就双手握拳。

这样做的目的是用小臂创造一个密封环境。身体前倾也是给攻击者发出一个 “顺从” 的信号，让他们明白您不是麻烦。以此来给自己的逃脱创造机会。

步骤2: 挣脱

请记住，越是死命扯，胶带就越是纹丝不动。您要做的是重新创造角度，这样才有可能撕破胶带。

要做到这一点，您要把手臂尽可能高举，高过脑袋，然后迅速地将双臂张开向两边下拉—— 就像是迅速将双手拉过两边髋骨那样。

故障排除

练习的时候，如果胶带没有破裂，很可能是因为您没有将手臂和双手分开超过两侧髋骨。

反复练习，直至掌握动作为止—— 从头顶开始，快速急剧下拉、分

开拉向两侧，超过髋骨。成功掌握了这个动作，胶带就会被扯开。

B 计划：如果您是从背后被胶带绑住了或者受伤了，怎么办

把您的手绑在背部的情况其实并不多见。因为绑在前面会更简单且更快，攻击者会倾向于选择以最快速度“制伏”您的方法。而且，绑在前面更方便他们扯着您的双手带您去任何地方。

不过，如果发生那样的事—— 被绑在背后了，或者您受了伤，没办法调整到扯破胶带需要的角度，那该怎么办？那就需要考虑B计划。

虽然方法不同，但目标是一样的，那就是调整角度，以撕破胶带。

[image]

这种方法需要您找到一个90度—— 墙角、椅子角、家具的拐角，什么都好，然后把被胶带绑住的手放在其边缘，做锯的动作，直至割破胶带为止。

如果决定练习这种方法，您可能会惊讶的发现，摆脱束缚并不复杂。

如果放任不管，胶带会侵蚀您的心理防线—— 而这正是攻击者想要实现的目标。

如果双手、双脚和嘴巴都被胶带缠住了，怎么办

建议您一步步来，首先尽全力挣脱双手。方法就是如上。接下来撕开嘴巴上的胶带，以便能正常呼吸，最后撕开脚上的胶带。

[image]
最主要的一点是要记住，不要让胶带和任何一种绑缚攻击您的心理防线，不要放弃。心理素质和技巧同样重要。

网上视觉资源很多。您可以通过搜索 “escape duct tape” 找到真人演示的视频。

[image]

如何摆脱束线带

虽然胶带是攻击者绑缚人质的常用方法，但束线带如今也是非常常见的。

束线带非常僵硬，如果不能掌握技巧，它极难逃脱。同样，它也会造成严重的心理负担—— 受害人很容易相信自己无法逃脱，从精神层面屈服。

步骤1: 调整姿势

被束线带绑住后，将双臂尽可能远地向身前延展，两臂紧贴。姿势就像您摆脱基胶带时那样。

步骤2: 旋转锁扣

您会看到绑住双手的束线带上有一个小锁扣。您现在必须转动锁扣，让它位于您的双手手掌的接合位置。

也无需把握得非常精准，只要能尽可能靠近中央位置即可。

显然，仅凭双手无法做到这点，必须用牙齿咬住束线带末端，然后将锁扣转到正确的位置。

步骤3: 挣脱

挣脱束线带的技巧和挣脱胶带是一样的—— 尽可能把双手向头顶高举，两臂紧贴，迅速将双臂垂直下拉，然后向两侧分开，超过髋骨。锁扣就会弹开。

故障排除

请注意！使用这种方法摆脱束线带需要比较大的力气，不是所有人都能做到。

下拉时手臂下落和双手分开都要按照正确的角度。如果角度不对，方法就不会奏效。

假如这种方法不起作用，也不要着急，记住还有另一种方法。

B计划：伞绳方案

所有人都可以摆脱布基胶带，但是要想摆脱束线带，对部分人来说并不那么容易。幸运的是，还有替换方案。

还记得在上一集中强调的准备工具吗？其中包括伞绳，这里就能摆上用场。

如果不方便在公文包或钱包里携带伞绳，可以考虑用伞绳替代鞋带。伞绳很好找，颜色各种各样，而且最重要的是，它看起来和鞋带没有太大区别。不会让您看起来奇怪。

把伞绳从包里或鞋子上取下来，理想情况下您需要七英尺长的伞绳—— 将它们穿过束线带，垂在双手的中央。

接下来两端各结一个圈，要大到足够把脚伸进去。

把双脚伸进伞绳圈，仰面躺下，用套在圈中的双脚做踩自行车的动作，这样束线带就能打开。

[image]

如何摆脱绳索

虽然绳索的运用并不像布基胶带和束线带那样普遍，但是如果发现自己身处极端险境，知道该如何摆脱绳索也是非常重要的。

步骤1: 调整姿势

被绑住之后，将您的双手手掌紧贴在一起，但手肘要分开—— 不要想被胶带绑住那样双臂紧贴。手肘分开的原因是靠手腕的弧度来创造额外的空间。

步骤2: 前伸和摇动

被绑起来后，保持手肘张开的姿势，将手臂前伸，直至完全伸直，同时保持双手端平，且互相紧压。

这样做之后开始迅速来回摇动双手，直至能够伸出一只手。

这种方法不论绳索粗细都能奏效，但是要注意，如果绳索很细，就像尼龙绳那样，花费的时间可能会更长，而且皮肉可能会被绳索割伤。

B 计划：用伞绳摆脱绳索

再一次，随身携带伞绳是个好主意—— 至少把普通鞋带换成伞绳。万一您遇到的攻击者擅长打结，那么这种方法就是一个很棒的备用方案。

这个技巧花费的时间也许比较长—— 需要30 ~ 50秒，所以，当您被单独扔在一个房间里面的时候才能使用这种方法。

在伞绳两端各结一个圈，将其从你的双手之间的绳索的中央位置穿过去。两个圈分别垂在绳索的两边。

把脚伸进圈中，仰面躺下，双脚做蹬自行车的动作，直至绳索打开。

您可以搜索 “escape rope” 选 “videos” 以找到演示视频。

如何摆脱手铐

手铐听起来很厉害，其实您真正需要的只是两个很便宜的小物件。如果您是女生，或者有妻子和女儿，那么您家里肯定有这种东西，那就发卡—— 弯曲的和条状的简易法卡。

方法1: 弯曲的发卡

前文在帮您挑装备的时候已经强调过，随身携带的工具之一就是发卡。这是很有用的。这种便宜的小东西很容易改造成能在几秒钟内打开手铐的工具。

步骤1 ：工具

如果能有套钳子的话会更简单，能把发卡精准地改造成想要的样子。

用钳子将发卡拉开成一条直线，发卡的一段本身是平滑的，另一段有锯齿纹，将发卡平滑的一端的小装饰点去掉，将平滑的这端稍稍向上弯曲。这里指的是大约1/4英寸长，弯成约45度角。基本就是个小铲子的样子。

步骤2: 摆脱手铐

为了使用这种方法，您需要使用右手。把手握起来，这样铐环的锯齿面就会垂落在底部（这部分在手铐封闭时是被扣在里面的）。您只需要考虑手铐的锁孔就足够。

锁孔是一个小圆圈—— 不要插入锁孔的圆圈部分，只插入小槽——让发卡嵌入小槽里，直至能感觉碰到了金属物。

一旦触碰到金属物，将发卡往下拉，然后向右。最重要的一点，注意这是两个不同的动作：一旦发卡到位了，先试往下拉，接着向右，L状路径 …… 不要尝试以一定的角度拉动，那样是打不开的。

故障排除

把发卡弯折出小的角度是完全能够做到的，只需要将末端向上弯折成小小的角，再试一次。

一定要先向下拉，再向右拉，这样就可以顺利打开。不要太用力，整个过程并不需要使用多大力气。

方法2: 条状发卡制作的垫片

步骤1: 工具

您需要的是基本款的条状发卡，啪的一声就能扣上的那种。这个工具

也需要您提前制作。

最终的目的是将发卡改造成一个垫片，能用来阻挡手铐锯齿部位，不让它们锁住。

首先要做的是将发卡从中段折断，只要向上弯折就能轻松折断。接着你需要折断发卡顶部较大的圆形部分。可以用钳子钳住这一部分来回弯折，直至断裂。

现在您就有了两个薄薄的金属片，它们的一端贴在一起形成一个“V”字形。V字形的开口处可能有些弯曲，所以用钳子将它们拉直。发卡的末端要尽可能直。

步骤2: 插入垫片

在这种方法中，只需要对付手铐中锯齿部位插入铐环的那部分。

拿出改装成垫片的发卡，插入锯齿嵌入铐环的那部分空间。将垫片按在锯齿上，接着迅速推到底。

往锯齿上按，一开始会给您推动垫片的冲劲。一旦垫片推到无法再推的地步，就在那里停住，接下来就可以提出铐环了—— 垫片阻挡了锯齿，所以无法扣紧，铐环因此打开。

您可以通过搜索“escape handcuffs using a bobby pin or a hair barrette”查找演示视频。

[image]

关于后备厢的挑战

这是一种非常刺激的挑战。

在掌握摆脱手铐的技术后，训练就会进入这一层面—— 实践在双手被铐住、头被蒙住的情况下，从封闭的汽车车厢中逃生。

这听起来似乎非常有难度，但如果您了解该怎么做，大多数人在几分钟内就可以完成逃脱。

如果您想冒个险，可以自己试试看。

首先是，别着急，慢慢行动。汽车后备厢非常狭小幽闭，置身其中的人会导致血压飙升，促使您感觉自己不得不加快动作。不要这样做！不能着急，着急会起反作用，要安抚自己慢慢来。

如果弄丢了弯曲发卡或垫片，在黑暗之中想要再找到它是很困难的。所以您应该集中精力，不要让紧张干扰到您的行动。

还要记住的一点是，所有新型轿车中都有能在黑暗中发亮的应急释放拉杆，找到这个拉杆应该不会太费力。但如果是被关在一个老式的车子里呢？

同样，不要慌。后备厢的锁不会特别牢固，您要做的是，四肢着地，用后背去撞厢壁—— 它可能会弹开，不过也将取决于车型。

那么其他选择呢？踢开后座。如果您最终要挑战这种方法，请先确保上述那些方法都已经尝试过了—— 而且还需要队友的合作，一旦遇到什么问题，他可以拉你出来。

搜索 “to escape when you’re trapped in the back of a vehicle” 选择 “videos”，以找到视频演示。

当被黑头套绑架 …… 现在该怎么办

您绝对应该尽一切力量击败潜在的绑架者。

现在不是抱怨的时候，而是要去踢、去撞、尖叫、利用一切可以利用的东西。

您需要知道的是：被绑架的前24小时至关重要。绑架者一旦得手，他们很可能会迅速转移您，有可能将你转移到安全的房间中，甚至转移多次，这样搜寻起来会更加困难。

[image]

您必须牢记，不论需要付出多少代价，一定要尽可能抢在前24小时内逃生。

除了转移的地理位置还不太远之外，这段时间内您的体力也最强。换句话说，肚子还是饱的，体内水分充足。如果超过24小时，这一切都会每况愈下，您的体力会大大减弱，逃生也变得更困难—— 绑匪绝不会给您足够的吃喝，他们需要您保持虚弱。

一旦局势明朗，您还无法击退袭击者，那就让自己表现得顺从一些。不要直视绑匪，低着头表演顺从—— 请注意！这是表演！仅仅是让自己看起来胆怯，尽可能避免绑匪对您实施额外的监管措施。在这种情况下您可以更容易择机逃跑。

如果被胶带绑住了，您大声尖叫，声嘶力竭，绑匪就会觉得您难搞，他们就会想把你塞进后备厢里，那绝不是您想要的结果，因为逃离后备厢会更难。

表现出顺从的同时，您应该尽可能快速思考自己可以如何逃脱。目标是寻找劫匪的安保方面的疏漏之处。瞄准机会，迅速下手。

[image]
[image]

如何撬锁、翻栅栏、短路点火发动汽车：反侦基础课 S06E05

[image] 关键词	地形侦查 救助 进攻 逃亡
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]防篡改准备 ；[image]突袭应对措施 ；[image]物理入侵检测
[image] 创建时间	2025年2月15日
[image] **Description**	行动安全性

特别强调：本集中介绍的技巧和方法，仅在您真的明白自己在做什么的情况下，再尝试和练习。S06系列的服务方向见总章节中说明。

- Table of Contents

  带刺铁丝网
  刀片铁丝网
  如何短路打火发动汽车
  合适的汽车
  打破车窗
  撬锁
  L形耙子和扭力扳手
  步骤**1:** 插入扭力扳手
  步骤**2:** 插入**L**形耙子
  步骤**3:** 找到第五根销
  如何防止入室侵害行为
  像入侵者那样思考
  策略**1:** 侦查周边地区

策略2 ：检查自家住宅
策略3 ：夜间侦查住宅

[image]

首先要说明的是，如果您只是为了练习就去尝试跳过带刺的铁丝网栅栏，不要这样做。这不是游戏。您可能会受伤。

但是，如果在真正需要逃生和躲避的境况下遇到这种情况，您首先应该知道该如何应对。

本集内容绝非推荐您用短路打火的方法启动汽车，因为那是违法的—— 除非是您自己的汽车，即使是这样，也不要轻易尝试，对汽车的损伤非常大。

但是您真的有必要了解其做法，这样一来，一旦短路打火发动了汽车，然后驾车逃离是唯一的逃命方法时，您就可以胸有成竹了。

下面我们逐一说明这些做法。

带刺铁丝网

需要的工具：在翻阅栅栏时，需要有一块厚重平整的东西，用来覆盖那些刺。

在紧要关头，您需要的是一条厚毯子、一张旧床垫、实在没有的话一块较大的特硬的纸板也能行。

该怎样做：您可能觉得翻越带刺铁丝网时需要万分小心，但其实没那么难。您可以找到任何东西遮住刺网，然后翻越那个覆盖面。

刀片铁丝网

刀片铁丝网的设计目的就是让人受伤，试图翻越者有可能严重割伤，进而流血不止而死 —— 至少逃不出太远。

曾经墨西哥边境上一名男子试图翻越这种铁丝网，反而被困在网中了。救援人员花了一个多小时才把他拉出来。这不是特例，仅一年之内就有21个人被这样困住。

除非有绝对的必要您再尝试这种，而且要极为小心。

需要的工具：一组人、拐杖或者其他类似的弯棍，一片平整的东西，就像翻越带刺铁丝网时用的那样。

该怎样做：这需要合作。队伍中派两名队员拿出拐杖或类似的工具，勾住刀片铁丝网，将铁丝网拉弯，直至变平。在这两个人保持拉平的同时，另外两人用平整的工具将铁丝网盖住，然后翻越。

等第一批队员翻越之后，换位工作；让第一批人用工具拉平铁丝网，覆盖，其他人翻越。

[image]

如何短路打火发动汽车

您真的应该希望自己不要碰到这种绝望的时刻—— 只能使用偷车的方法逃跑。这可不是电影。

再次重申，不要在自己的汽车上练习这种方法，这会导致汽车受损。

合适的汽车

首先您需要挑选一辆合适的汽车，可以在危机的情况下短路打火启动的汽车。看看四周围，有没有没锁门的汽车，或者钥匙扔在座椅上的马大哈。

当然，找到没锁门的汽车是中大奖了。拖车有一套万能钥匙，可以让您进入周围所有轿车。如果一眼望去周围没有拖车，也找不到没锁门的汽车，那么接下来您只需要选择老款车，1999年及之前的那种车子。

实际上如今老款车依旧很多，在路上驾驶时留意一下，您能找到一大把。

需要的工具：

- 钢丝钳和剥线钳
- 钳子
- 一字型螺丝刀
- 锤子
- 绝源手套
- 绝缘胶带

该怎么样做：过程非常简单 …… 也许您可以放一套具体说明在身边，以防危急情况。因为这个技巧极难在平日练习，文字指南防止您在慌乱的情况下忘记具体方法。

1、找到可以短路点火启动的车子之后，将一字螺丝刀像插钥匙那样插入点火装置；用锤子将螺丝刀往里推；转动螺丝刀，就像转钥匙那

样；如果转不动就用钳子帮忙。运气好的话这样就可以发动汽车。

2、用螺丝刀起开驾驶杆上下塑料板上的螺丝；挪开塑料板，您会看到下面有几根电线。

3、找到两根红线圈，它们是供电线圈。

4、戴上绝缘手套。

5、割开两根红线的末端，然后用剥线钳剥开绝缘皮。将两根红线的末端捏在一起—— 请注意，是您刚才割开的两根红线一根一边，不要把同一根线拧在一起，那样不行。

6、找到棕色线圈，它是负责连接打火器的。有些车子只有一根棕色线，有的车子有两根。

7、将两根棕色线都割开，从尾端剥开。

8、如果有两根棕色线，将两根线搭在一起，启动汽车。车打燃后，不要让线圈再接触，必须将它们分开放置。可以用绝缘胶带缠起来，避免触碰。这样也能避免您触电。

如果只有一根棕色线，将这根棕色线搭在两根红线上，打燃汽车。车子启动后，将线圈各自分开，用胶带缠住棕色线的末端。就像上面说的那样。

打破车窗

如果需要打破车窗逃生，而且不被人觉察，那么基胶带就能派上用场。

多撕一些基胶带，在车窗上贴成 “X” 形状。这样能防止玻璃溅得到处

都是，尤其是能 降低噪音 。

另外，使用战术防身笔或者类似的工时，记住，要击打玻璃的角落，不是中间，角落是玻璃最紧绷的地方，也更容易击碎。

[image]

撬锁

开锁工具套装并不贵，用起来也很有意思。如果您能遵循下面的说明，万一哪天朋友和邻居忘带钥匙了，您可以帮个忙。

并没有太复杂。如果您花5 ~ 10分钟练习，锁不会损坏；但如果您练了几百次 …… 那个锁就够呛了。所以，如果您需要每天练习2小时，请选择那种对您来说不重要的锁。

L形耙子和扭力扳手

开锁需要的全部工具就是一个L形耙子和一个扭力扳手。

开锁最难的地方在于，使用扭力扳手时您需要找到正确的的压力角度。如果施压过大，锁就会觉得像是受到了侵犯，拒绝打开。要施加最小的力度。

基本来说，每次您觉得力度合适了，都只能施加其十分之一的力度。

所以，当您在按照下列步骤插入扭力扳手时，请记住这一点。练习越多您就越熟练，越容易找到合适的感觉。

步骤1: 插入扭力扳手

强调，将扭力扳手插入到锁底的时候，一定要轻。把扳手的长柄松在一边，将手指放在扭力扳手上，一定要将力度降到最小。

步骤2: 插入L形耙子

注意，在撬锁的整个过程中，扭力扳手上的施加力度都必须保持一致。如果力度增加，就不会成功。

将L形耙子插入锁孔，脊部朝上。在来回刮耙子的同时，也稍稍向耙顶施力。

把L形耙子想象成牙刷，您就像是在给锁刷牙 …… 就像那样的动作，在锁中进出。

步骤3: 找到第五根销

注意，当您哄住了锁，让它相信五根锁销全都操纵到位之后，锁就可以成功打开了。

很常见的情况是，头四根销只需要几秒钟就可以打开，接着需要改变行动，找到第五根。

为了找到第五根锁销，需要改变L形耙子的使用方法。

现在将耙子上下猛拉，一定要确保依旧是将锁前后探到底。当碰到第五根销时，你就感觉到扭力扳手的压力，接着锁就开了。

这可能需要花点时间练习。一旦找准感觉，懂得如何操控工具，您只需要几秒钟就能打开它。

挂锁和档案柜都适用。

您可以搜索 “pick locks” 在网上寻找相关视频。

[image] 世界顶级黑客 Kevin Mitnick 的名片。您可以看到，这张名片折叠起来就是一个撬锁的工具。

如何防止入室侵害行为

[image]

返回 - 相关自卫措施：[image]防篡改准备 ；[image]突袭应对措施 ；[image]物理入侵检测

入室侵害的犯罪率一直高居不下。以下是美国联邦调查局的统计：

- 有1/5的家庭会成为非法入室侵害的受害者；
- 85%的窃贼会在入室侵害之前先侦查情况；
- 50%的窃贼在行动之前会伪装成服务人员，比如快速、维修等等；
- 94%的窃贼在行动之前处于兴奋状态；
- 30%的暴力袭击发生在入室侵害案件中；
- 60%的强奸发生在入室侵害案件中；
- 33%的窃贼是通过没关严的窗户和大门闯入的 ……

还有一种从来不会被官方统计的入室侵害行为，那就是警察亲手干的 —— 有没有搜查令都是事后才会被问起的。 本系列重点考虑这种 。

像入侵者那样思考

再一次，就像躲避追踪者、防御网络攻击那样，您需要采取对抗性思考方式，像敌人那样思考。这样您就可以弄清自己的家在这类恶意入侵的威胁中是否有薄弱点。

策略1: 侦查周边地区

第一条策略其实非常简单，那就是在您家附近走一圈，同时，您需要仔细观察。

您发现了什么？哪个房子看起来有人居住？就在此刻看起来像是有人在家的样子？哪个房子看起来像没人在家的样子？注意寻找这样的信号。

观察信箱、报纸、快递纸箱等出现的情况；垃圾堆在门口吗？还是门口积满了尘土？门把手上有塞着小广告吗？…… 您肯定知道自己居住的地方有哪些特征能证明一扇住户门后是否有人。

您在等快递包裹吗》

签收快递时要非常小心，这一点至关重要。伪装快递的入室抢劫是很常见的，在全球常见。

正规的递送都需要事先电话联系您，如果没有电话或类似的约定，就不要开门。

[image]

返回 - 镇压手段：[image]敲门

物流公司很容易检查快递人员的身份，以及您的包裹的单号，您需要心中有数；如果是其他朋友寄东西给您，需要事先和那位朋友沟通

好，了解递送公司和单号，大致的时间等细节。

任何时候，不要仅凭一个人穿着制服或声称他自己为某家公司服务，就轻易相信他。

在中国，小区住宅门的把手上经常会被塞上小广告，是那种塞在那里的，而不是贴在墙上或门上的；如果房子里面的人开门力气过大，那些纸有可能被震落。如果一扇门上被塞了好几张小广告，且多日内仍在那里，也许说明房子里没人。

不要小看那些小广告，也许它们是某种标记。当您看到那种东西时，请及时把它扔掉。

在纽约，窃贼使用黑胶布来做同样的事—— 他们偷偷把一块黑胶布贴在目标住户的窗户玻璃上。如果几天后黑胶布还在那里，说明这间房子里没有人，他就会按计划行窃。

在爱尔兰，窃贼用粉笔做标记。都柏林和利默里克经常出现那种粉笔标记符号，不同的线条代表不同的意思，比如："好目标"、"太危险"、"没什么价值"、"有钱人"、"有警报器"、"已偷过" …… 甚至还有对房子主人的描述，比如 "紧张害怕"、"脆弱女性，容易骗"，等等。什么样的线条代表什么意思，窃贼团伙的人自己明白。

相信其他国家也有类似的现象。总之，您需要做的就是，留心您的住宅出现的小广告和罕见的标记，及时清除它们，这一点对保护家人安全来说至关重要。

策略2 ：检查自家住宅

再一次，对抗性思考方式—— 像入侵者那样思考，仔细观察自己家里有哪些地方是薄弱环节？如果有人从这里/使用这种方式闯进来，怎么办？

在您家里和周边转几圈，注意每一个有可能藏人的地方；尤其是有院

子的住宅，您需要确保如果院子里有人，您和邻居都能够立刻看到，一览无余。

还要注意那些透露了您家里装满值钱东西的信号。炫富是非常危险的事哦！不论在线还是现实中。

车道上停着一辆价值不菲的汽车吗？由于忘了关上百叶窗，在外面的人一眼就能看到超大的平板电视和昂贵的电脑吗？您曾经在线与他人分享位置吗？在社交媒体上晒过奢华的休闲生活吗？ ……

并不是说您不应该享受香车美食和高级家电，而是您应该保持警惕，不要把财富秀给潜在的罪犯。

安全大原则：任何时候，陌生人对您的了解越少越好。

策略3 ：夜间侦查住宅

如上所述，白天侦查已经可以受益良多，夜间重复这一过程也非常重要。

绕行住宅四周，思考如果自己是窃贼，可以怎么做？如果有人躲在垃圾桶的区域后面或者灌木丛里，你能发现吗？哪个角落太黑以至于藏了人也难以分辨？您家周边的灯光够亮吗？如果有入侵者靠近，您可以及时发现吗？……

[image]

就像检查网络和电子设备的安全性一样，您需要特别注意薄弱环节。

[image]
[image]

在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

[image] 关键词	个人 反监视 防御
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]反监视
[image] 创建时间	2025年2月16日 13:00 (GMT+8)
[image] **Description**	行动安全性

什么是敌对监视？如何为此做好防御？

本站资源主要为敏感人士及前线社区的安全防御服务，包括活动家、记者、人权维护者、人权律师等等，不论意识形态。事实上任何人都应该对防御知识有所了解，尤其是在极端化盛行的动荡年代。

- Table of Contents

  逃离监视
  监视预防
  阻止措施
  规避演习
  反监视小技巧：

[image]

虽然大数据时代人们越来越多地谈论的是技术监视，但不可否认的

是，依旧有很多时候人力监视是被重点使用的 —— 敏感人士对此应该颇有感触。人力监视有很多便利，比如更直接、易于调度、稳定、杂音少等等，监视者们很清楚这些便利。

很多反侦查技术涉及监视检测和特殊保护操作 —— 不论您需要防备的是流氓还是警察，在此都一样。您完全可以将其应用于您自己的生活中，培养自我保护意识，对威胁信号保持敏锐觉知。

[image]

返回：[image]如何检测您是否正在受到监视：监视检测和特殊保护行动

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

返回：[image]暗中监视的迹象

观察的技能对于防御来说是至关重要的，并且您可以随时随地应用。具体取决于您关心的是哪些资产（人员、财产、信息、声誉和贵重物品）以及如何更好地保护它们。

这绝非鼓励您在一些偏执的安防泡沫中生活，肯定不是，没有人想要以这种方式生活。了解恶意行为者和当权者的隐蔽操作中使用的策略并不意味着您必须自动实施它们。但扩展您的知识和提高您的意识可以帮助您做出更明智的安防决策。

想想看，例如，为什么家门上贴着防盗报警贴纸的住户往往很少被破门而入？这是因为敌对的监视人员倾向于将这样的房子排除在潜在的目标列表之外，而不是那些看起来更容易闯入的房子（可以考虑在您的门上贴这类贴纸，即使您没有装报警系统）；还有一个原因可以解释为什么您会发现更多的被窃汽车案例发生在汽车停在墙边或大灌木丛前面的时候，而不是在私人住宅前面。因为这些区域可以令敌对监视人员的操作比较顺利、风险较低（最好避免将车辆停放在墙边、灌木丛或空地一整夜）。

如果您是敏感人士由于政治原因而成为目标，上述贴纸和汽车的情况尤其需要您警惕。因为这种情况下您所面对的不仅仅是财产损失的问题了。当年的斯塔西曾经干过这种事 —— 他们偷偷潜入目标人的家和汽车，悄悄地移动更改一些布局、藏起一些东西（比如相框、衬衫或一只袜子），并不拿走任何财物。多次下来会令目标人陷入怀疑自己精神错乱的境地，失去斗志。想想看，如果您某天回家时发现原本应该在北墙上的全家福现在挂在南墙上、原本刷干净的碗碟里居然有血迹……

这种情况下大多数人（包括无神论者）都会陷入困境，会被强大的疑惑压垮、陷入不可自拔的自我审查。这正是敌对监视人员所希望的结果。

我有两位朋友的汽车行李箱被撬，失去了重要的东西。这在他们看来是一个完整的谜。他们当时并没有让车子停放很长时间，周围也没有其他车辆被闯入，尤其是，窃贼是如何知道哪辆车子里有值钱的东西呢？

很简单，受害者此前长期遭受着秘密监视而对此一无所知。监视者看到他们把什么放入了行李箱，并尾随他们抵达一个“容易下手的地方”才开始撬门的。

上述这些都属于敌对监视。敌对监视的应用非常广泛，不论是图财、图色、恐吓、操纵还是实施心理压力。顺便提一下，如果您必须在汽车后备箱中存放物品，请事先查看您周围的环境以确定安全。

还有一个重要原因是，敌对监视者通常首先在社交媒体上关注他们的目标，然后接近受害者的住所和工作场所，开始跟踪他们，找到他们的规律和弱点。这是一个典型的敌对计划过程 —— 被称为社交媒体情报的一部分，其中敌对计划者最初从现有的开源信息中提取他们想要的东西，然后转换到静态监视，继而转向移动监视。

可以继续举出更多这样的例子，但基本的信息都是相同的：即 学习如何从不同的角度看世界，对于防御来说是至关重要的。

延伸：https://iyouport.substack.com/p/2df?utm_source=publication-search

延伸：https://iyouport.substack.com/p/fa3?utm_source=publication-search

延伸：https://iyouport.substack.com/p/--194?utm_source=publication-search

[image]

返回 - 镇压手段 ：🕷人肉搜索

如前所述， 了解自己在一个间谍眼中的样子，是很重要的。了解地方和人 – 包括您自己 – 如何能够出现在潜在的敌对观察者身上，然后改变您的行为方式，以便改变敌对计划者用来评估您的风险/收益的平衡 。

这可能听起来像是高技术性的，斗篷和匕首之类的东西，但真的不必担心，大多数防守动作和战术几乎是可笑级的简单。

但必须说，仅仅因为它们很简单并不意味着每个人天生都具有如何保持安全的知识。常识并不总是那么常见的，至少对于那些从未真正停下来思考它的人来说，不会容易。

说到共同点，在此我经常能得到一个可预测的反对意见，即 教育人们关于监视、监视检测和保护性操作，这真的对吗？透露防御技巧会不会反而帮助’坏人’提高了技能呢？或者会不会提示坏人想到如何绕过防御的办法？

好吧，对于第一个问题，答案就是“坏人”在敌对监控方面通常不需要太多帮助。他们对此早已非常娴熟，相反，一无所知的人是他们的目标，也就是那些“好人”，因为他们从来没有任何理由去思考或体验这些东西。

获得技能主要是提高您的防范意识和威胁敏感度，并获得一些经验——大多数“坏人”已经做过的事。他们还会继续做下去，现在您有必要了解这些事。

至于第二个问题，答案也是否定的。为敌对计划者配备有关保护性操作的一般知识并不能真正帮助他们绕过或逃避安全措施（只要信息不太具体。传授这些知识的人肯定有分寸）。

这是因为关于目标的一般知识并不能消除恶意计划者最终出现在目标区域的需要（以便收集更详细的信息）。正是在这点上，作为安全专业人员，我们可以阻止、检测、承认或调查潜在的敌对监视者。

敌对监视者在规划和监视阶段的相对脆弱性就是反监视防御工作的利益所在，以及，一旦您理解了事情的运作方式，检测和阻止它们就会变得相对简单。这些漏洞是所有敌对监视所固有的，即便他们了解安防措施也很难克服或绕过这些漏洞。

再一次，“坏人”早已知道这些，因为他们是在平衡高风险情况方面经验最丰富的人。“好人”是那些需要了解周围发生了什么的人。

下面简单说说防御敌对监视的一些技巧。

[image]

逃离监视

首先要明白的是，监视本身并不是您应该担心的最大威胁。监视只不过是一种信息收集工具，所以，最值得您警惕的东西应该是您的对手最可能关注的信息。

在开始之前有必要澄清，没有任何文字能自称在实际程度上教会任何人彻底逃避监视，想要成功需要学习者亲自去做很多的练习，因为这里很多知识都是隐性的，学习者需要在经验中领会并将知识体系补充完整。

还有必要说一句，在安全问题上，没有任何客观的权威，永远都有很多不同的方法可以达成既定的防御目标。本站中很多内容来自世界各地的反抗前线多年的经验，也许还有更多人在其他方面也有类似的经验。所以，如果您是团队培训师或学习组织者，请务必重视队友们的反馈和经验交流，收集起来并仔细分析，进而不断扩充和深化本站搭建的安全体系，以令更多朋友受益。

好消息是，人力监控是一项相当棘手的业务，这意味着除非您正在与一些很熟练和专业的敌对监视者打交道（比如情报机构 – 国安部），否则通常不需要花很多时间就可以摆脱他们，大多数外行监视者都很容易被甩掉。

接下来看看您可以采用的一些策略，以保护自己免受敌对监视。我们将从一些更基本的常识方法开始 —— 实际上非常有效的方法。然后介绍点更性感的东西。

监视预防

大多数人都会有这种防范的下意识。每当您避开城里某些危险的地方、或者决定不在夜间走入一条黑暗的小巷时，您基本上就避免了多数罪行发生之前的简单监视。如果您长期坚持采取安全措施并减少各种足迹残留，您将首先降低被定位和被跟踪的风险。

此外，外出时最好保持低调。豪华轿车、昂贵的服装和华丽的玩具等等都可以让您脱颖而出，成为暗枪的目标。我曾经告诫很多人关于低调的重要性，但不能否认他们通常甚至没有注意到这一事实 —— 因为“调”是不是足够“低”当事人自己不敏感，敌对监视者可是非常敏感的。

以下是一些最简单的措施（还有更多措施）可以帮助防止被监控。您可以把它们融入意识，更主动和自然地实施：

1. 尽量改变您的日常行程和旅行路线。请记住，仍然会有一些您无法改变的例程（上下学、接孩子、上班工作等），但是仍然

可以使用一些变动进行随机的调整，只要您想这样做。

1. 尝试通过与您进入的门不同的另一扇门离开。在商场、酒店、火车站等较大的地方，这将更容易做到。但您也可以在许多学校、办公室、公寓楼甚至住房中找到一扇后门。

1. 尽量避免在静态监视位置进行重要行动，这些位置可以从安全距离（街边咖啡馆和餐馆、公园、城市广场等）轻松监控。
BACK [image]如何检测您是否正在受到监视：监视检测和特殊保护行动

1. 当您与某人见面时，尝试约在室内（咖啡馆、商店、酒店大堂等）您能轻松检测周边环境的空间，碰面后快速离开约见地点，而不是直接在原地交流。也尽量不要花很长时间在街头等人。使用[image]户外无设备对话 原则时尽可能看走边说，尽可能不停在一个固定的地方。

大多数人可能没有意识到这一点（很可能因为没有亲自做过监视者），事实上如果您不急于逃跑而是原地呆上数小时（比如在咖啡馆里静坐），可能就会阻止一个不那么忠诚的监视人员坚持下去。不要低估监视的繁琐程度。如果对方的预测是您很急于离开此地，那么您采取原地静坐的方式是最理想的，会让对方怀疑调虎离山。除非您正在与一个真正的专业人士打交道，或者只是一个非常专注的对手，否则您通常可以简单地摆脱他们。真的不是什么华丽的方法，但它可以非常有效。

阻止措施

我经常发现，当敌对监视被发觉时，很多人会自动采取“斗篷和匕首”的方法 —— 试图秘密侦察和反击。这在某些情况下可能很重要，但一些明显而简单的方法可能会更有用。

您可以让周围的人清楚地了解您所处的环境，简称就地联合。如果您觉得有人在监视您，您可以直接盯着他们看。如果您盯住一个地方

看，周围的陌生人就会纷纷对这个位置好奇，这样就能把监视者置于一个尴尬的境地。

您甚至可以通过手机拍摄来跟进。根据情况（如果这样做是安全的话），您甚至可能想要面对他们，问他们是谁以及他们想要什么。切勿让他们跟踪您到某个重要的地点、或者对您来说可能不太安全的区域。

这些是传统的常识性措施，并不会因为我们能想到更棒的措施就可以忽视这些基本的方案。

为了避免您认为这种做法只适用于低级别的情况，我可以举个例子：以色列安全局的一名前成员（通常被称为Shin Bet），他在以色列大使馆负责间谍工作时就采用了这种方法，在90年代初。来自一个敌人国家的三名特工常常占据餐厅的一张桌子，这张桌子的角度可以清楚地看到大使馆，这是静态监视的重点位置。以色列人举着一只大相机来到餐馆玻璃窗外，对着那张桌子边的人猛拍了几张照片，然后就回去了，此外什么也没做。那之后再也没有看过那些特工出现。

规避演习

我知道这可能听起来很奇怪 – 您怎么能摆脱您没有先检测到的东西？

答案是无论有没有检测到监视，您都可能会以同样的方式摆脱它，所以，不管有没有检测到监视，只是采取一些规避的动作是完全没有害处的。可能只需要几秒钟或几分钟。您显然很想要检测自己是否受到了监视，但如果没有大量的培训和经验（通常情况下都是如此），这可能是一项艰巨而耗时的任务。那么，即便成功检测到监视您依旧要采取相同的规避行动，那么为什么还要等那么久呢？

理解规避行动的关键是首先了解监视的工作原理，了解其困难并利用其漏洞。

您可以利用的机会是监视人员不会直接看到您的短暂时段。当您开始

移动时 —— 从静态监视转入动态，这种时段几乎总会发生，因为监视人员还必须关注目标要去的地方，同时还要保持一点距离，让目标先转弯停一点时间再继续跟踪，等等。

在这里您可以利用的漏洞是监视者难以紧密跟踪目标（特别是在拥挤的区域），这将导致他们自然倾向于锁定某些视觉线索（外观、高度、移动方向等）。于是可以通过快速改变某些变量来对监视者产生视觉干扰，从而打破他们期望看到的线索。

以下是一些有用的东西。

反监视小技巧：

1. 建立缓慢、稳定的运动速度，可以从舒适的距离轻松监控的那种状态；

1. 然后，忽然改变状态。在您前面的某个地方寻找一个可以让您突破监视视野的位置 —— 即使只是几秒钟。这可以是转弯、进入百货商店、火车站、酒店等，提前对该地区有所了解可以将其效能提升到更高的水平 —— 老练的监视人员通常知道不能在目标人长期居住的区域下手，因为那里的地形对目标有利；

1. 充分利用这一短暂的监视盲点，迅速改变尽可能多的视觉变量（外观、肢体语言、步速和运动方向等等），监视者此前努力建立起的监视线索将被消解，他们会开始发愣。

介绍一个有趣的例子。这个例子并不涉及真正的敌对监视器（它是在防御课程上的演示），但这更具挑战性，因为对手是五个非常专注的监视人员，其中大部分都有多年的特种部队、执法和维稳经验。

目标走在市中心的街头，穿着一件蓝色系扣衬衫、带着一个深色背包。目标首先确保自己保持缓慢的步伐并将自己定位在宽阔的人行道中间，以便五个特工更容易从远处跟踪。

这个图景可以令监视人员陷入一种舒适的、甚至有点自满的距离和节奏。当目标最终到达一个地铁站附近时，忽然变速，迅速走下楼梯转过拐角。立刻就获得了几秒钟的监视盲点。

目标利用这几秒钟飞快跑起来，并迅速脱掉了衬衫，把它塞进背包里，然后戴上背包里准备好的黑色棒球帽和眼镜。然后迅速从街对面的出口离开，采取正常的步速，融入了人流。

此时监视者还在努力寻找“蓝色衬衫和黑色背包的男子”。在繁忙的地铁站和拥挤的商业街，这种手法很好用。只需要**10**秒钟。

这一思路和专业魔术师所做的并没有什么不同 – 将他们的观众导入虚假的期望，重新引导他们的注意力，他们就看不到您的诡计。

[image]

对付人力监视者的方法大多是如此，即 从人的心理弱点下手。记住他们是和您一样的人类，您的弱点他们大多都有，通过日常观察自己的弱点便可以计划出很多类似的防御策略。

机器监视没有“心理弱点”，但要知道，通过机器监视操作的也都是人，是人在通过机器获取的信息进行决策，于是如果您确定基本监视者是机器，那么有可能更容易解决。

[image]

返回 - 镇压手段：📹偷拍 ；[image]隐蔽的监视设备 ；[image]视频监控 ；[image]物理监控（上岗） ；🚁空中监视

的确，基于人工智能（AI）的监视一直在增加，通过允许政府和执法机构跟踪任何公民，实现了真正的技术反乌托邦。但是，对于每种技术，都会引入一种可以欺骗它的方法。

比利时 KU Leuven 大学的一组学生在 arXiv 上发表了一篇论文，包括如何借助简单的印刷图案轻易地欺骗用于识别图像中人物的AI系统。

只需要将一个特别设计的花纹/图形，放在身上，就可以让您无法被AI检测到。这种图案如果印在T恤上，穿上它你就可以隐身了，当前的自动监控技术无法检测到您。

对于普通大众来说这可能有点奇怪，但在AI的世界中，这些模式被称为对抗性示例，它使用的是计算机视觉系统的脆弱性。

其实对抗性示例已被用于欺骗面部识别系统。在这里看到视频：

https://youtu.be/MIbFvK2S9g8

这里指的对抗性示例只会欺骗 YOLOv2 算法，但包括谷歌在内的各种科技公司开发的现成计算机视觉系统使用的都是YOLOv2。此外，如果一个活人正在查看图像，这种方法是无用的，您依旧需要上述对付人类的办法。

最后，还是那句话：练习。练习非常重要，任何技巧和技术只有通过不断练习才能真正变成您自己的东西，才能在您需要的时候发挥作用。

[image]
[image]

特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06

[image] 关键词	个人 反监视 街头 逃亡
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]反监视 ；🕷人肉搜索
[image] 创建时间	2025年2月16日
[image] **Description**	行动安全性

想要抵制政府间谍的侵害，就要学会像政府间谍那样思考，以看清自己的薄弱环节，并及时修补。

从普通周旋到高级对抗，有一些基本技巧。

- Table of Contents

  敏锐的态势感知
  专业间谍会注意以下情况：
  在汽车里被监视
  如果发现自己被监视了，现在该怎么做
  策略**1**：停下来转身
  策略**2**：宣告知情
  策略**3**：不做软弱的目标
  策略**4**：待在公共场合
  如果发现自己被监视，为了确保安全，需要注意以下事项：
  策略**5**：减速、混淆视线
  当您遇到高级威胁时
  改变行动习惯

极端监视
平行监视 ——
跳蛙式监视 ——
迷惑监视者 ——
团队监视 ——

[image]

在行动之前，恶意者一般都会跟踪、观察或监视他们锁定的目标一段时间。绝大多数绑架、抢劫和入室行窃案的受害人都在此之前受到过监视，时长从几分钟、几小时到几天或几周不等。

[image]

返回 - 一个著名的安全事故：[image]当您准备像编程随想那样工作…：须知

于是您应该知道，学会摆脱监视、迅速判断自己是否被人跟踪并甩掉跟踪者，是防止侵害的关键。首先以最快速度意识到自己被跟踪，这样才能争取到足够时机采取行动以保证安全。

现在您应该已经了解监视有哪些类型了，最基本的应该知道：跟踪、偷拍、有目的的社交媒体情报收集、包括黑客入侵，有些时候他们不仅针对您本人，还会针对您周边的人，您的亲密关系、家庭成员、要好的同事和朋友等等。

[image]

返回：[image]给活动家的反人肉指南

如果只有您一个人在防御监视跟踪，那会非常吃力 —— 需要假设为敌方的人越多，压力就越大；更好的办法是，让您身边更多的人掌握如何识别和摆脱一般监视的方法。当每位队友都能具备这样的基本意识和能力的时候，群体安全就能实现了。

敏锐的态势感知

您需要做的第一步就是以最快速度判断出是否有人在跟踪您。这里必须重申第一集中介绍的基本态势感知意识。您需要准确判断哪些信号不正常。

其实没那么难。·

比如您是一位女士，在一家大型商场里选手袋。您忽然发现不远处有一位男士神情奇怪，看起来不像是对手袋感兴趣，他的眼睛一直在瞄向周围的人，包括偷偷瞄向您。

您会意识到这种奇怪的“关注”，我们每个人都有这样的直觉，很多时候只是您还没有激发出它、或者您的注意力被恶意操纵了。

在手袋区闲逛的男士本来就不会很多，这是基于常识的信号；但这一信号究竟是否能说明出现了问题？您只需要使用一些技巧来测试它。

首先假设这一初步判断是准确的。您可以通过快速转到其他购物区来进行观察。如果对方真的瞄准您了，他肯定会跟随您到下一个购物区，甚至再下一个区域。

这就是情报界使用的概测法：

- 一次＝意外
- 两次＝巧合
- 三次＝敌对行为

当然，如上面的例子，那个男人有可能是在帮助女朋友或母亲购买礼物；为了排除这点，您就需要采取探测策略，当第三次转换区域后依旧发现他的存在，那就不再是巧合了。

正如前面曾经介绍过的那样，试图行凶的家伙会从跟随您的步速开始，这是很容易判断的指标。

一般情况下毫无用心的陌生人会下意识地避免与您同样的步速，您可以稍微留意下这点，如果两个陌生人出现了相同的行进速度，其中一个人必然会变快或者变慢，以错开同步。但是跟踪者却不会，他们将始终追求与您同步 —— 不论是汽车还是步行。

于是这就是一个很容易判断的指标。

[image]

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

为了确保不被监视，您需要格外注意、保持警惕。

专业间谍会注意以下情况：

1、在街上有人靠您太近：正如前面提到的，意图行凶者会跟随您的步速，如果您小步走，他也会小步走以配合您的步伐。您需要注意这点。

2、有人与您对视：一般正常人不会在街上死盯着另一个人看，当出现目光相对时，正常人会立刻错开目光以避免不舒服；但如果有人这样盯着你，请小心，这可能说明有事要发生。

3、有人似乎对您太过关注：如果有人多次在您的日常路线的同一地点、同一时间出现（比如下班途中、放学途中、公交车站、健身房等等），监视这个人，注意他的行动。

不要低估自己的不适感，诸如不安、焦虑、疑惑、怀疑、犹豫和恐惧。

如果以上情况有一项或多项出现，您就有可能已经被监视了。

[image]

支持日常更多使用**S01**中的练习题，以调试并维护您的压力水平和心理健康程度，以便保持敏锐，并做出正确且快速的响应。

比如：[image]S01E01-T3 创伤经历如何影响您的认知 ；[image]S01E05-T2监测自己的压力水平 ；[image]S01E06-T2 找到弱点建设新的防御能力

在汽车里被监视

在您开车的途中也非常有可能被跟踪。你可能会注意到有一辆从没见过的汽车开过您的小区；在通勤、去杂货店或回家的路上可能看到有辆汽车和您一起转弯；或者有时看到有人开在您前面，接着变换车道，然后它又出现在您身后了。

[image]

要做到这样的观察能力，最重要的是记忆力。平日就要有意识地多多练习。

为了确认是否被跟踪，您可以采取以下办法：

如果是在公路上，先下车，比如假装打电话，然后再回到车上。重新上车后请注意，那辆车还在后面吗？有意识地减速，那辆一只跟在后面的车也同时会减速吗，保持和您同样的速度？比如您一开始以75英里每小时行驶，那么就减到60英里。

这种情况下没有意图的其他车辆会迅速超过您；而有意图跟踪您的汽车会跟随您的减速而减速，以保持它自己始终在您后面。当然，这是只单一的跟踪者，如果是团队行动的政府间谍，他们的同伙车辆会在下一个路口跟上您。

[image]

如果发现自己被监视了，现在该怎么做

仅仅判断出监视还不够，必须面对跟踪者。

情报人员有5种简单的策略可以用来反监视。这些方法您也可以使用，您不必具备多年侦查经验，也可以使用它们。

这些方法便于实施。能帮您拜托严重的危机。

策略1：停下来转身

当有人跟踪您的时候，停下来转身的方法很管用，它既可以帮助您判断是否被监视，也能让对方知道您已经对他的行为有所警觉。

如果当时您在行走，那只需要停下脚步转过身，假装有事要做——比如查看电话、系携带、或者假装转身找人。

接着，直视您认为正在跟踪您的那个人。

一般外行的跟踪者在此时就会方寸大乱。他可能会被吓呆，或者至少表现不自然，因为您在攻其不备。这就很容易识别到了。

换句话说，跟踪您的人不可能表现得像街上其他路人那般自然。

策略2：宣告知情

正如前面所提到的，一旦判定自己被跟踪，很重要的一点就是，让对方知晓您已对其行为有所警觉。

一旦潜在的危险被察觉，多数坏人都会放弃。记住，坏人是在寻找理想的施暴对象，宣告您已经意识到他们的存在、知晓他们想要加害于你，此举将让您变得不再是那么适合下手的对象。

策略3：不做软弱的目标

换句话说，您不应该成为“理想的施暴对象”。您需要展现出强大的一面，挺直腰背走路，把头抬起来。给一个人打电话，谈论有人在跟踪您，声音要大，动作要明显。

不要担心，把战术防身笔掏出来，准备好使用它。

坏人在视野内挑选施暴对象时他们选择的都是那些看起来懦弱的、或者看起来掉以轻心的人，比如低着头、塌着肩膀。

策略4：待在公共场合

如果确定被跟踪了，一定不能回家。

表面上看起来家似乎是安全的地方，可以锁起门来打电话求助，但是，这种情况下一定不要这样做。因为坏人会强行闯入，或者假装离开，其实是隐藏起来，计划着晚点时候闯入。

如果发现自己被监视，为了确保安全，需要注意以下事项：

1. 待在人多的地方，公共场所，打电话求助。比如餐厅、咖啡馆、拥挤的街角等等地方；

1. 永远不要走入黑暗的小巷或无人的街道，在那里您会与世隔绝，坏人会更容易对您下手；

1. 如果在公共场合被跟踪，例如杂货店。不要走出店铺返回车上。几乎所有坏人都会等在出口处，等您走出来；接下来他们就会跟踪您的车，或者尾随您回家。

策略5：减速、混淆视线

如果确定有车辆跟踪您，继续驾驶 —— 再次强调，不要回家 —— 改变车速、多转弯，让跟踪者意识到您已经产生了警觉。

情况安全的时候，请注意跟踪车辆的车牌和汽车型号，记住它们；要能做到在下一次识别它们，并且求助时会非常有用。

当您遇到高级威胁时

[image]

高级威胁指的是，威胁来自那些对您了解太多的人。

也许您不知道恶意者在此前如何对您进行了侦查，因为您不认识他们。除了谨慎使用互联网之外 —— 避免发布任何关于您自己的真实信息 —— 您还可以通过分身方法来阻断监视侦查的路径。

[image]

返回 - 自卫措施：分身

并且您尤其应该注意那些可见的高级威胁，比如愤怒的 Ex、充满怨恨的前同事或雇员、欠下巨额债务的熟人 …… 或者，每次锻炼完健身房外都有个人在注意您吗？某个人总是和您同时去那家店买东西

吗？等等。

如果按照高级威胁来应对，有一些重要的附加防范措施需要注意。

改变行动习惯

如果担心某个特定的人会跟踪您，那就需要注意您一直采取的习惯性行为模式。

这一点可能有难度，因为人类都是习惯的动物，很难打破常规。但是为了安全，打乱行为模式以及活动顺序是至关重要的。

- 改变早上出门的时间
- 改变通勤路线和时间
- 打乱行为。如果每天在同一家店吃早餐，那就换一家，或者选择不同的时间
- 去之前从未去过的地方购物和用餐
- 下班后挑选不同的回家路线

需要注意的是，这些策略的确可以让您难以被跟踪，但是不要忽视提高警惕；不要离开黄色态势感知 —— 黄色能让您远离不得不正面对抗的红色态势，即 危急情况。

[image]

极端监视

这种情况指的是您面对那些非常专业的政府间谍或私人侦探。如果您是重要的政治敏感人士、让政府焦头烂额的人，您需要警惕这种情况。

平行监视 ——

需要的工具：

- 两辆或更多的汽车
- 道路信息—必须有平行道路

如何行动：第一辆车跟踪目标，保持一定的距离；另一辆车从与目标行驶车道平行的道路上跟踪目标。一旦目标车辆转弯，另外那辆车就能接替监视。

跳蛙式监视 ——

需要的工具：

- 多辆汽车
- 暗语

如何行动：这种方法需要多辆汽车和随时保持联系的对讲机。您和您的搭档需要创造出一套用于描述目前状况的暗语，避免对讲机信号被监听。

正如其名所示那样，这套监视方案需要通知前面的搭档，目标正在靠近。这就意味着第一辆车无须减速或撤退，无须向目标隐藏身份。

迷惑监视者 ——

摆脱监视者最好的方法就是给他们捣乱。

给完全陌生的人随便传句话，或者走进商店，开始漫无目的地闲聊。这些简单的行为就足以迷惑监视者，甚至甩掉他们。

团队监视 ——

需要的工具：

- 一组人
- 对讲机
- 周边区域信息

如何行动：实施团队监视需要将一组人马安插在目标可能出现的战略位置。这些人需要通过对讲机进行联系。

如果行动位置是一个大城市，你可以将组员安排在地铁入口、街角、还可以是目标停留的酒店或咖啡馆。监视团队的每个队员都通过对讲机提前通知彼此目标的位置。

[image]

非常建议您练习一下想象力，想象自己如果在这种环境下被跟踪，你可以如何甩掉目标。如果您身处险境，知道该如何保护自己也能让人充满力量。

从现在开始，对身边人保持警觉；注意那些在商店里和您一起排队的人；观察餐馆里盯着您看的人；对那些与您保持着同一路线的车辆不

要掉以轻心。

意识到这些人的存在，正是保证自己的安全需要走出的第一步，保持自信和警觉，这是能救命的。

[image]
[image]

警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A

[image] 关键词	反侦察 反监视 对抗性思考方式 逃亡 隐姓埋名
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]隐姓埋名 ；[image]S04完美隐身-总章节：机智是重要实力
[image] 创建时间	2025年2月16日 9:00 (GMT+8)
[image] **Description**	行动安全性

知己更要知彼。

- Table of Contents

追踪者的困难是逃避者的机会
基本搜寻方法
1、总是从采访有信息的人开始。
2、私人物品，尤其是数字设备。
3、追踪者需要制作一个目标人的行为档案。
4、绘制数字档案（样本档案）。
5、社会关系图。
6、线索串联。
7、时间是最危险的东西。
8、系统化的大数据。

[image]

故意躲起来的人是最难找的，因为他们会精心设计很多避免被找到的方法；被绑架藏匿的人是次级难找，因为绑匪会精心设计避免被找到的方法，但被绑架的人（如果足够聪明的话）会努力留下被寻找到的踪迹。相比下迷路的人更容易被找到。

但不论如何，找人的工作采用的都是一套相似的方法/思考方式，只是在深入程度上有所不同，不论是警察还是NGO组织，都依靠近似的逻辑。

本站S04系列“完美隐身” 是在藏匿者角度上的思考。本集则反过来，作为对抗性思考方式，帮您了解对手会怎么做，以便有针对性地准备。

想要追踪您的人都懂得一些基本的追踪原理，他们知道该如何查找线索。那么这些线索是什么呢？

追踪者的困难是逃避者的机会

追踪者会从目标人的失踪原因开始，做一些简单的排除法 —— 关于此人最不可能去的地方，以及更可能去的地方。

“相关人员”是追踪者入手的第一步：亲戚、朋友、同事和其他熟人。每个人通常对情况都有自己的看法，对所发生的事情有各自的叙事版本。这些版本越是混乱，追踪者的耗时就越长。

追踪者需要获得基本信息（故事情节），否则将没有任何线索和初步数据。而这一阶段，上述“相关人”会提供很多错误的信息以及情感参与。追踪者必须花很多时间把真相和事实与人们的猜测区分开。如果没有最详细和真实的故事情节，就很难向前推进。

追踪者定期需要与相关人员进行沟通，不可能通过一两次对话得到成功搜寻所需的一切。额外的问题总会出现。情绪激动的人经常会提出一些不存在的东西。

对逃跑者来说，您身边的人对您的了解越少，对您的失踪越是毫无准备，追踪者就会在此更多碰壁。

有目的地失踪者在失踪前通常会大大混淆追踪线索，比如销毁电脑、手机，烧毁各种文件，删除社交媒体账户，清除电子邮件，等等。所有这些也会使调查变得更加困难。

[image]

返回：[image]大清洗 - 扫荡危险区域：完美隐身 S04E07

对于追踪者来说最重要的方面是预算。在这种情况下追踪者真的需要大量的费用：向不同的机构、计费系统、城市监控摄像头、交通系统（火车、飞机等）等提出信息要求。成本会因国家而异；对于逃避者来说，也取决于您得罪的人有多大的权力，权力越大，他们可用的预算就会越大。

[image]

任何寻找失踪人员的行动都有一个重要规则就是：如果一个人失踪造成的损失远远低于寻找他所需的预算，那么就没人愿意去找这个人。

有许多不同的“但是”，如声誉或“原则问题”，这些是相当例外的。否则，预算就是主要的规则。这一原则并不适用于寻找亲戚或朋友。当然，也有例外情况，即有可能不计成本地追踪一个人，但这种情况极少发生。

基本搜寻方法

每个案例可能都是独特的，但有一些基本原则对任何搜寻来说都是一样的。

1、总是从采访有信息的人开始。

大多数情况下，这些人是失踪者的亲属和朋友。

有必要尽可能详细地重现当时的情况：事件在失踪前后发生的顺序是什么？谁是最后一个见到失踪者的人？失踪者当时的行为上是否有任何不寻常？失踪的动机可能是什么？该人是否带走了什么东西？等等。所有这些都是初步信息，追踪者可以在此基础上进一步开展工作。

2、私人物品，尤其是数字设备。

追踪者会想尽办法检查失踪者的记录、电话、电脑和其他东西，如果它们还在的话，失踪者的家属一般会允许这样做，因为他们会被告知这样才能更快找到人。

对于失踪者来说，您留下什么东西，需要心里有数， 甚至可以用故意留下的东西来误导追踪者 。

例如，浏览器的历史记录，或者有趣的信件等等。一般来说，访问通信工具和社交网络中的交流对追踪者来说都是非常有价值的信息。

3、追踪者需要制作一个目标人的行为档案。

为了做到这一点，他们会仔细分析社交网络、视频、照片，有时还会分析手写文本。有时它是了解失踪者动机的重要关键，同时，也可能让追踪者能够部分预测目标人的行动。

4、绘制数字档案（样本档案）。

包括全名、年龄、婚姻状况、工作地点、社会关系网络、爱好等等。一般来说，这是一份关于个人的经典分析报告。这也可以帮助从另一个角度审视目标人的个性，因此可以揭示各种有趣的事实。

5、社会关系图。

追踪者需要特别注意失踪者所处的环境，有必要明确描述“关系圈”。很多时候一个人不可能什么都不说就消失。通常，失踪者的关系圈内至少有一个人知道一些信息，但由于各种原因（承诺、害怕什么、试图混淆调查，等等）而不说话。

对于失踪者来说，您应该知道，近亲是最可能被追踪者密切关注的。

6、线索串联。

在所有这些步骤之后，追踪者必须将收到的信息系统化，并绘制出事件发生的时间线。可视化工具是这种情况下的理想选择。例如：Gephi。

老方法当然也可以，就是在白板上做标记，红线、贴纸和磁铁。它被称为“侦探板”。这种方法适用于旷日持久的调查。

请注意，如果您是追踪者，在推进调查的过程中要时刻记得所有的新数据都必须输入您的图表中。

7、时间是最危险的东西。

有时，搁置反而是好办法，可以帮助追踪者推进调查。因为随着时间的流逝，人们往往会犯错和放松，失踪者在最初的几个月内会格外小心，而过了这段时间就会觉得自己安全了，这种情况下就会下意识地泄漏线索。曾经有一个目标人在失踪六个月后，在商店付款时使用了自己的旧信用卡，这一点是严重错误的，他立刻就被抓到了。

[image]

紧张和疲惫是失踪者最大的障碍，预算和时间是追踪者最大的障碍。在这里，谁能拖垮对方，谁就能赢。

8、系统化的大数据。

追踪者的工作就是系统化能够采集到的一切数据，以进一步应用必要的操作 —— 例如：查看城市监控摄像头，要求银行提供账户报表，目标车辆的移动情况（如果失踪者有车的话），他是否购买了机票、火车票或汽车票，是否越过了边境，确定手机的位置，以及其他数据。这一切都取决于追踪者具体的能力、权力范围、以及身边有多少专家。

警察做的事都是一样的，只是，通常，由于他们的工作量和官僚系统的一些特点，要慢得多。于是如果您遭遇的不是当局，而是私家侦探，可能会更麻烦，因为私家侦探没有官僚主义，机动性更强，更不择手段。

当然，每个案例都是独一无二的。本集内容给出的是一个框架，任何追踪调查都在这个框架内，但您必需灵活变通，有些时候传统方法是最适用的，而另一些时候，您非常有必要创新技巧。

从追踪者的经验上看，在大多数情况下，调查到了一定阶段就会陷入死胡同。原因有很多：预算已经耗尽；当事人离开了这个国家，在某个地方追踪者没有关系可以接收信息；入手太晚，最初成功的机会不大，还有很多其他原因。这些追踪者的麻烦就是失踪者的机会。

[image]
[image]

武器和自我防御的重要策略：反侦基础课 S06E08

[image] 关键词	反击 搏击 街头 街头战术
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]反攻
[image] 创建时间	2025年2月18日
[image] Description	行动安全性

从身体状态到武器，从准备到运用；您需要、也只能通过反复练习才能掌握要领，仅仅阅读是不够的。请记住，尽可能不要打架！战斗是为了找到逃生机会，绝不是袭击他人。

- Table of Contents
万不得已的搏斗是为了寻求逃生机会
情境1：有人抓住您的胳膊，想把你拖走
情境2：你被人从身后抱住
情境3：袭击者抓住了您的头发
情境4：被锁喉
情境5：有人要对你重拳相击
关于挑选和使用武

器方面，您需要知道的
1、战术防身笔
1.1、挑选合适的战术防身笔
1.2、握笔
1.3、战术防身笔放在哪
1.4、利用战术防身笔
1.5、利用防身笔抵挡拳头
2、携带刀具时您应该知道的
2.1、遇到持刀攻击时怎么办
2.2 步法矩阵
2.3 前进三角
2.4 后退步法
2.5 侧向行动和绕中心旋转
2.6 了解更多刀具防御知识
3、 保持最佳状态

[image]

[image]

返回：[image]街头搏击基本技巧（转帖）

掌握防身技能并不需要您无所不知，精炼几个简单的技能就可以抵御大多数威胁。本集将提及的情境都可以用类似的技能应对。

强烈建议您每天抽出几分钟来做练习，最终您会发现，这些技能可以信手拈来，达到完全自如的状态。

您可以先挑选一项做开始，等到运用自如时再继续其他技能。当然，希望您永远不要碰到危险，如果一旦碰到，这些技能将可以拯救您的

生命和心爱的人的安全。

万不得已的搏斗是为了寻求逃生机会

这是一个大原则。

当您具有足够的能力时，也应该尽可能不要将自己置于需要搏斗的境况下。因为那样将产生很多后患。搏斗应该是在不得已的情况下的防御。

您需要做的是尽可能降低危险程度，还应该注意，即便搏斗，您的目标也应该是为自己创造逃跑和求援的机会。

这就是为什么 **ETGS**（**escape to gain safety**）应该作为第一个策略提出，它是当您受到侵袭时的基本行动。方法如下，适用于大多数情况：

- **E** 指代眼睛（**eyes**）：看准目标，瞄准攻击者的眼睛戳或刺，动作要快；

- **T** 指代喉咙（**throat**）：您可以瞄准攻击者的喉咙、喉头和声带。攻击此处会令对方向后倒。

- **G** 指代腹股沟（**groin**）：如果您正面面对袭击者，也就是他在你的面前，那就踢他的腹股沟，用全力。

- **S** 指代小腿骨（**shin**）：反复踢打攻击者的小腿骨，那个地方相对脆弱。

下面将介绍的是处于更危险困境下的应对方法，以防万一。

不过要记住的最重要一点是，尽可能快速离开事发现场，不要被吓得呆住；还有就是如您看到的那样，控制危险。这两点都很重要。

情境1：有人抓住您的胳膊，想把你拖走

将这个策略教给您的孩子也很有用 —— 所有人都应该清楚，如果某人抓住您的胳膊想把您拖走时，应该如何应对。

首先您需要反抗。虽然这时候的自然反应是后退，但是后退会让您陷入与袭击者的拔河比赛。而且您可能赢不了。

相反，这个时候您应该做的是前进 —— 突然抬起手肘砸向袭击者的脸。抬起肘部猛击能突破对方对您的手臂的控制，这样做您更有可能安全逃生。

如果是年纪较小的儿童，或者瘦弱矮小的人遇到了强壮的袭击者，如果无法抬起手臂以摆脱对方，那就用另一只手紧紧抓住被袭击者控制住的手臂。两只手一起用力成功的可能性会更高一些。

情境2：你被人从身后抱住

假设您正在徒步，或慢跑，忽然有人从胡同里或灌木丛中钻出来，从身后将您抱住。这种情况下不要向前跑，您需要大步后退以打破袭击者的平衡力。

与此同时掰开对方的手指，可能的话用大力气将其掰断。

如果您能对他的手伤害程度足够，他就会放手。此时可以用手肘攻击其颈部。或者转身踢打其腹股沟，接着趁机逃跑。

如果袭击者想通过后仰然后以将您抱离地面的方式举起来，可以用腿

勾在他的腿后部，这样他就无法将你抱紧。接下来再用上述方式，从攻击其手指开始，以便找到逃生机会。

https://youtu.be/gC6GU3488zQ

情境3：袭击者抓住了您的头发

从正面：这种情况女性比男性更值得担心，但需要知道，即便头发很短，也可能被拽住。如果有人从前方逼近您，并抓住了您的头发，要知道这个位置其实很便于您的反击。

因为他在您前面，您可以很清楚他的动作；并且您也知道，抓住您的头发的那只手不能再发起攻击。

所以可以借机攻击对方，记住**ETGS**：眼睛、咽喉、腹股沟、小腿骨。

一旦摆脱了对方的控制，尽可能快地往人多的地方跑，一边大声尖叫。基本上对方就不敢追上来。

从后面：如果头发被袭击者从后面拽住，这种姿势下您看不到袭击者，但可以很清楚他所处的位置。重要的是，不要急于摆脱；相反，靠上去，抓住他的双手，用最大的力气死命抓住；然后开始旋转，同时还要抓紧不要松手，直至看到他的手臂向后弯折。

此时就可以掰开他的手指，然后采取上述ETGS准则攻击他，找到机会逃走。

情境4：被锁喉

有人想掐死你，这显然是严重的危机，需要立刻逃脱。这里所用的技能也适用于攻击者用威胁的方式抓住你的衣服。

这项技能超级简单，但是非常有用。

为确保在需要时懂得如何实施，你应该留意脖子上有凹陷的位置。照镜子自己看下。这个位置非常脆弱，也正是你需要攻击对方的位置。

当这个人的双手掐住你的脖子时，你需要迅速伸出两根手指狠命地刺向对方脖子的凹陷处 —— 被猛戳这个位置的人会被呛住，会弯腰后退，你就可以趁机逃跑。

https://youtu.be/8HgoLLezD14

情境5：有人要对你重拳相击

出拳的速度会非常快，您可能不一定可以做到更迅速应对 —— 尤其是当您的状态比较放松时。于是，您能做到的防御就是，不要让自己进入放松状态。

并不是说一直紧绷，而是，如果有人接近您的私人空间（以您的身体为中心半径为一臂的范围）您需要警觉起来，把手稍稍抬起，最好准备。

不要带有威胁性，您可以通过其他动作做遮掩，比如拿着手机或报纸，或者端着杯子等；流露出威胁性会令事态升级。

中小幅度抬起手，可以竖起一道屏障，当需要的时候就可以更快速做出反应。

如果对方抡圆了手臂、挥舞着拳头朝你走来，你需要做的是双臂向上弯曲，这样当他挥拳打过来时，你可以猛砸他的上臂。

现在你处于优势地位，可以转身面朝袭击者，向他的颈部砍过去。可以继续攻击，也可以逃跑 —— 记得要朝准袭击者的枕骨凹痕处出击，这样能让对方完全丧失方向感。

如果拳头朝你直接打过来，你需要使用的技能有些许差别。

如果感到有危险，你需要抬起手臂（再次提醒，不要表现出威胁性，以免使事态升级），提至约肩膀的高度；当拳头径直打过来时，就弯曲前臂，这样对方的拳头就正好落在你的手肘尖上。

重拳砸到手肘会给袭击者造成极大的伤痛，这种策略很容易折断对方的手指。如果想了解这是什么滋味，想象你的拳头在用最大的力气砸向餐桌的桌角。就是那样。

一旦袭击者砸中你的手肘，趁他痛苦的时候你就可以迅速发起攻击——采取上述ETGS准则，或者干脆逃生。

https://youtu.be/4npb2uZpMGs
https://youtu.be/IKa5t7xVbNw

关于挑选和使用武器方面，您需要知道的

“If a fight is inevitable, you have to hit first”

1、战术防身笔

正如前面几集中所讲过的，战术防身笔很重要。因为您可以把它带到任何地方，包括乘坐飞机，以及进入任何禁止携带刀枪等武器的地方。

战术防身笔看起来完全无害，但它不是普通的钢笔，它更厚重，材质是航空级铝合金，最重要的是，它的低端有一个尖角。不要担心，您不会被这个尖角刮伤，也不会破坏您的衣服和包，但这个尖角可以造成严重伤害——当它被猛戳出去时。

这种笔非常坚韧，不仅可以用来反击，而且可以在必要的时候砸破窗户以逃生。

1.1、挑选合适的战术防身笔

不论您购买哪一款，都需要确保考虑以下事项：

- 质量取胜—购买所有武器的经验法则；
- 应该有一个能用以攻击的坚韧的金属尖；
- 应该有笔夹，挂在裤子口袋或裤子内部（如果放在手提袋里无法及时拿出来就没什么用了）；
- 笔盖的尾部应该扁平，可供紧握住，而且这样可以把大拇指放在笔盖上，以增加攻击时的力量；
- 以及，书写流畅，可以换墨水，能供长期使用。

1.2、握笔

使用战术防身笔时首先要知道如何正确的握笔。

正手握笔是可行的。关于正手握笔，可以想像持刀剑刺向某人。

但是您会发现，这种握笔的姿势实际上没有太多的控制能力，想要给对方造成严重打击会更难。

而反手握笔能让你更加自如地控制防身笔，进攻时会有更大的力量。别忘了把拇指放在笔盖顶端，这样可以有更多的支撑点。

1.3、战术防身笔放在哪

这一点也非常重要。要让它发挥作用，您就不能在身处险境时再到处找防身笔。

根据您的左右手习惯，您可以放在顺手一侧的裤子口袋里。您需要能以最快速度拿出防身笔。

不论放在哪一侧，您需要通过练习构建肌肉记忆力，以便条件反射般地明白该去哪里取。

1.4、利用战术防身笔

分为3个简单的步骤：

1. 握住防身笔；

1. 将笔直接抽出；

1. 将笔直接刺出（几乎就像拔枪一样）

假设自己身处不同的险境，练习使用防身笔；训练自己在不同的模拟情境下抽笔，例如站立、仰卧、行走中、逃离防线或事发地时、被某人从后面抱住或袭击者正面走来的情况下，等等。

如果无法在上述所有情境下都能顺利抽出防身笔，那么您就需要换一个放笔的位置。找个朋友一起练习是个好主意。

1.5、利用防身笔抵挡拳头

前面已经介绍过如何应对重拳相击，现在防身笔又为您增添了一项工

具。

每当感觉周围奇怪时 —— 比如步行经过黑暗的小巷、身处混乱的酒吧或餐厅、有人用奇怪的眼神看向你时 —— 做好准备，握紧防身笔。请记得，每次都需要以降低事态危险性为目标，而不是让事态升级，否则对您没什么好处。

把防身笔小心地握在手中，让其靠近小臂上，这样可以避免被潜在的袭击者看到。如果对方抡圆手臂打过来，就用前面说到的技巧，抬高手臂抵挡拳头；然后用另一只手 —— 握住防身笔的手，瞄准袭击者的腋下或胸肌刺过去，这样对方很容易受伤。

如果拳头直接打过来，您还可以转动握笔的手，让防身笔朝上，这样袭击者的拳头就会砸在笔尖上，他会痛不欲生的。

2、携带刀具时您应该知道的

一如既往，您应该先考察一下本地的法律，关于是否能携带刀具进出哪些设施。其次，您需要选择最合适自己的款式。

以下几条事项，您应该先考虑清楚：

- 准备把刀放在哪？腰带上？口袋里？
- 您喜欢穿什么样的衣服？如果平时穿牛仔裤比较多，就能应付刀身的粗糙；
- 边角。如果您总是穿西装，那么它可能会划破衣服，您需要选择带有光滑手柄的刀具；
- 如何运用刀具？手动款、还是自动弹开式的？

- 它能承受多大重量？它能有多大尺寸？

不要忘记练习，这一步至关重要，能帮您了解如何正确的抽刀运用，以便在遭受袭击时可以不假思索地加以运用。

挑选日常也能携带的刀具很重要，不能在紧急情况下再思考“今天带的刀是什么来着？”那就麻烦了。您应该随时都知道自己携带的刀具的情况，且明白如何运用。

2.1、遇到持刀攻击时怎么办

以下是当碰到有人持刀攻击你时能帮您逃生的办法。

成功的防御刀刺训练以三角形为基础，所有动作都要呈角度进行；用刀具进攻的整个过程中，唯一能直接上前的情况就是，当你狠狠地抵在攻击者背上时。

https://youtu.be/0gfE_y6vPGw

2.2 步法矩阵

要练习这个步法，您可以找一卷电工胶带，在地板上贴出一个大大的“X”形状，然后再在中间加一道横线，形成一个巨大的*星号。

这样，无论你想要前进、撤退、还是侧向闪躲，该符号都能为您提供指导，帮你避开事发地。

2.3 前进三角

前进三角能让你拥有更多的可能性，因为你可以一边闪躲一边进攻。你的脚步与迎面而来的威胁呈45度角。

这种步法非常简单。如果向左进，那就先移动左腿闪避；如果向右进，那就先移动右腿。

你会移动到能避开威胁的侧面。

这一步能让你处于可以避开袭击者攻击的位置。同时，这种步法也把你带到能造成破坏的地方，接着退回以躲避攻击。

它还有一个附加的好处，如果需要狠狠撞击袭击者，这个位置也能让你的臀部更有力。

只要记住，用这种步法后退和前进时都要保持平衡。

https://youtu.be/tfmZcz3z-r4

2.4 后退步法

你也可以用同样的45度角退出中心位置，以远离危险。

只需要练习将身体舒适地前进和后退，习惯这种步法的感觉。一旦遭遇危险，您很可能没有时间去考虑该怎样行动。

https://youtu.be/yq9TZXp8O9w

2.5 侧向行动和绕中心旋转

如果危险从正前方直接逼近，你也可以向两边闪躲。向侧面移动，然后转身，迅速将身体背转过来。

2.6 了解更多刀具防御知识

您也许可以找一家正规的培训中心，他们肯定会教会您如何在自动取款机前被刀抵住后背时怎么办、遭遇劫车被刀抵住喉咙怎么办等情

况。

正规的训练至少需要有以下这些内容：

- 无论刀具抵住的是您的喉咙、胸膛还是后背，你都能够令袭击者缴械投降；
- 如果袭击者利用方向盘的杠杆原理来劫车，你能够制伏他；
- 如果有人一直藏在你的车后座 —— 包括在行驶途中，你可以如何制伏他；
- 如果有人趁你熟睡时进门，用刀抵住你的喉咙，你也应该能够让其缴械；
- 如果有人持有致命武器，如何攻击其要害部位例如肱动脉、颈静脉、心脏，或者通过剖腹来发起反击。

这些只能通过实地训练获得。也许可以在网上找到不少视频。但是依旧需要亲自尝试才能掌握要领。

https://youtu.be/eC-2X_6BCEU

3、 保持最佳状态

身体状态是非常重要的。

日常训练其实很简单。它的目标就是，如果遇到灾难，您不至于跑出10步就疲惫不堪。如果必须背上72小时工具包走几里地，您不应该有任何问题。

您也必须能摆脱短期危机，如果在停车场遭遇绑架、在小巷里遭遇抢劫，您需要能够迅速逃离危险区域，进行有效的自我防御。活动家走

在街上避免被套上黑头套也需要这样的爆发力练习。

下面这些简单的练习就能给身体积累爆发力，让你能在遇到危机时快速行动。计划：

周一：高强度训练。全速奔跑15～30秒，紧接着暂停60秒。

全速的意思就是全速，用尽全身最大的力气，在这15～30秒内如果没能到气喘吁吁快要瘫倒的地步，说明您还没有用尽全力。

按照这个模式练习5次，接着走上一公里来平复。

周二：轻松地跑 3～4 公里，这次是慢跑，但肯定会出一身汗。

周三：重复高强度练习。5组 15～30秒全速奔跑，每次间隔休息60秒。最后走一公里来平复。

周四：又一次长跑，慢跑 3～4 公里。

周五：再次高强度训练，重复周一和周三的内容。

当然您可以随意更改。如果您此前很长一段时间没有练习过任何内容，那么建议从减量的程度开始，以便让身体熟悉节奏。然后在加量。

训练能带给您自信心，帮助您变得更加冷静和敏捷，更好的体力是逃生的关键。试试看吧。

[image]
[image]

如何在大规模枪击案中幸存：反侦基础课 S06E09

[image] 关键词	枪击
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法
[image] 创建时间	2025年2月20日
[image] **Description**	行动安全性

希望您永远不要遇到这样的事。

- Table of Contents

  1、准备好
  2、主动意识
  3、观察人群
  4、在事情发生之前确定潜在的出口
  5、识别可用做掩体的所有物体或屏障
  6、确定潜在的隐藏点
  7、确定可以用来自我防御的潜在武器
  如果听到枪声怎么办
  跑—躲藏—战斗
  1、跑 —— 远离枪击者，以最快速度抵达射程之外
  2、隐藏
  3、不建议装死
  4、为生存而战
  其他建议
  培训视频

[image]

“大规模枪击事件” 的定义各不相同，但通常被定义为 3 ~ 4 人被杀的枪击事件。然而也可能的状况是，许多人遭到枪击受伤，但没有人死亡，仍然可以定义为大规模枪击事件。

这可以来自于所谓的恐怖组织、也可能来自于 “报复社会”，或者纯粹的精神病态，再或者，针对抗议者的镇压行动。

[image]

返回：[image]如何处理枪伤：街头实战指南 S05E04

似乎没有任何一个公共场所能够幸免于大规模枪击事件的危险。学校、教堂、电影院、KTV、商场、百货公司、餐馆，甚至健身房、广场 …… 随时都可能会发生毫无意义的悲惨事件。

所以您需要一些基本层面的防御技能。

1、准备好

以下是一个清单，关于您需要做点什么以便能让自己应付可能发生的大规模枪击事件。

生存的宗旨就是 —— 最好在任何事情发生之前进行战略性思考，并制定计划。这里也一样。如果您发现自己正处于射程范围内，您已经没有时间去思考该怎么做，因为每一秒钟都事关生死。

诚然，每一种情况都是不同的，但有一些普遍适用的生存策略，您值得了解。

2、主动意识

如果是暴力镇压导致的大规模枪击事件，也许不难预测到；但是如果

不是这种，其他任何一种都是很难预测的，因为它们随时可能发生，而且在任何地方都可能发生。因此，合乎逻辑的假设是，它可能在任何时间任何地点发生在你身上。

所以，防御的第一步就是要更加注意周围的环境 —— 即 态势感知。当您在公共场合时，请密切注意建筑物，比如出口入口、可以藏身的房间，或者可以藏身的东西，比如比较大的金属台等等。进门时先扫一眼四周，让自己心里有数。

3、观察人群

您需要注意的是任何看起来可疑的人。寻找任何穿着可能用来藏匿武器的长风衣或背着大背包的人。

这里需要使用到的是在现实中反侦察的技巧，见下面。简单说，您需要知道您的观察应该瞄准什么样的细节，对于那些不得不随时躲避政府间谍和线人的异议人士来说，这些技巧都非常有用。

[image]

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

总之，您的观察力越强，反应就能越快。即便是错了也总比保持沉默让灾难发生要好得多。

这并不是说让您保持绝对的偏执状态，而是强调您应该警惕什么 —— 目标是明确的，那就是保命。也并不是说每一个穿着大风衣的人都是坏人，只是一个简单的事实是，在风衣下很容易隐藏武器，所以您需要密切注意。

4、在事情发生之前确定潜在的出口

每当您进入一个公共场所，首先应该做的就是确定出口的位置 —— 寻找任何可以离开房间或建筑物的方法，在脑子里记住它们。

除了门之外，还要寻找窗户甚至天花板上的出口。在弗吉尼亚理工大学发生的大规模枪击案中，一些学生从二楼的窗户跳下，逃到安全地带。

这是为紧急情况做好准备的最基础建议。在每一次乘坐商业航班时，您都会被提醒要首先确定所有出口门的位置。

5、识别可用做掩体的所有物体或屏障

您需要寻找的是砖墙、水泥柱、自动售货机、钢门或金属门。普通的桌子、椅子和大型盆栽植物都不能提供足够的掩护。

6、确定潜在的隐藏点

如果现场的状况导致您无法接近上述已经观察到的出口，那么躲藏可能是下一个最佳选择。

在您确定了所有潜在的出口后，就要继续寻找潜在的藏身点。寻找一个房间或衣柜，尤其是有门锁的房间。

记下这些藏身点的位置，并为如何快速到达那里规划出一条路径。

7、确定可以用来自我防御的潜在武器

接下来就是要确定潜在的武器了。如果您不能跑，也无处可躲，战斗就可能是唯一的选择。

寻找任何可以变成武器的东西 —— 如拖把或扫帚柄、一把剪刀、可

以扔向枪击犯的重物，甚至是可以扔出或点燃的有害化学物质。

您应该把这些东西的位置记下来，以便在需要的时候可以及时抓住它们。

[image]

返回：

如果听到枪声怎么办

如果听到枪声或听起来像枪声的声音，就应该立即采取行动。您所做的准备工作到此为止，现在需要迅速做出决定。

当枪击事件开始时，有一件重要的事情要记住 —— 枪手是为了在最短的时间内杀死尽可能多的人。在大多数情况下，他们并不在乎发生什么，因为他们已经做好了在屠杀结束时自杀的准备。

当一个枪手进入一个设施并开始射击时，混乱将会爆发。人们会尖叫和奔跑，这时一般很难迅速做出决定。您最好是事先在心中有一个计划。

跑—躲藏—战斗

身处主动枪击事件中的人需要记住这句简单的话，“跑，躲，打”。

下面将更详细地介绍其中的每一个字。

1、跑 —— 远离枪击者，以最快速度抵达射程之外

逃跑是听到枪声的自然反应。枪击案的现场视频画面中，人们常常会向四面八方散开以避免中枪或被杀。如果能跑，就跑吧。尽快离开该地区，但需要尽量保持对自己所做的事的认识，乱跑只会增加危险性。

在一些事件中，受到惊吓的人们实际上是向拿枪的人跑过去了。当时一片混乱，没有人真正知道发生了什么。

您需要的是尽量保持低调，以不稳定的模式运动。这将使您成为更难对付的目标。如果可能的话，尽量躲起来，从一个掩体跑到另一个掩体。尽量往出口方向跑。

2、隐藏

如果您无法离开枪击现场，那么下一个最佳选择就是隐藏。寻找潜在的藏身之处，比如寻找一个带锁门的房间。

如果无法跑到另一个房间去，那就找一些物体躲在后面，比如墙、柜子、桌子、大的柱子等。寻找任何可以遮挡住您整个身体的东西，并且要足够厚，可以防弹的。

您需要寻找由重金属制成的家具、橱柜和其他结构。避免使用铝、木头和其他轻质材料制成的东西。这将有助于保护您免受枪击，并帮助您躲避枪手的视线。

尽量保持警觉，并准备好在必要时转移到其他地点。

尽量保持安静。尖叫和/或哭泣只会引起枪手的注意。如果可以的话，将手机静音。

一旦您进入可以藏身的房间，就需要立刻用能找到的所有重的东西堵住门。

将您能找到的最重的物品移到门前，防止门被撞开。在某些类型的门上，您可以在顶部的铰链上系上一条皮带，以防止铰链延伸。

如果可能的话，关上灯。请记住，枪手们都在寻找快速和简单的杀伤力；如果有其他光线充足的地方有更容易的目标，他们一般会避开黑暗区域。

只有在必要的情况下才用身体挡住门。因为如果门不够厚的话子弹可以穿透。

3、不建议装死

不建议 “装死”，除非您已经别无选择。一些大规模枪击案的受害者选择了装死，救了他们的命；但是，在其他情况下，枪手会回来对着尸体射击。

只有在您没有其他机会逃跑、躲藏或战斗时再选择装死。

4、为生存而战

在这种情况下，您真的是在为自己的生命而战了。这里没有规则，也没有所谓的干净的战斗。攻击者有武器，而你没有。

如果可能的话，在枪手瞄准您的时候弯腰、以低位的姿势快速朝向枪手冲过去以把对方扑倒。

- 去抢夺枪支。如果别无选择，请尝试抓住武器并将其从枪手手中拿走。如果可以，将武器尽可能远地扔开，然后再跑。当您逃跑时，请不要拿着枪，因为其他第一响应者可能认为您是枪手。

- 搏击 —— 踢、抓、咬 …… 以任何可能的方式让枪手受伤。

- 用指甲抓他们的眼睛；踢他们在腹股沟；揪住他们的头发 ……
- 一边搏斗一边大声喊叫，以最大的力气喊叫，巨大的声响可能会使枪手迷惑。

其他建议

1、社区、学校或工作场所有都必要组织一些专门的培训，关于应对枪击案的逃生指导；如果有相关培训，请参加，现场的培训非常重要，是文字无法描述清楚的实操。

2、您最好能习惯于随身携带一些隐秘的武器，具体建议见本系列第3集[image]您必备的基本防身装备：反侦基础课 S06E03 ，尤其是，您应该在日常进行一些练习，以便能够顺手地使用这些武器。

3、最好结伴而行，最好与同等应变能力的朋友结伴。没有时间争辩和思考，您需要迅速评估状况并采取行动。

培训视频

如果您实在找不到现场培训，可以看一下视频讲座，以便帮助理解这些技巧。

以下视频提供了有关如何应对积极的射手并在大规模射击中幸存的建议。

1、来自 NBC

https://youtu.be/qWFanYD3cgo

2、来自ABC

https://youtu.be/4rl-XCQev1g

[image]
[image]

如何检测您是否正在受到监视：监视检测和特殊保护行动

[image] 关键词	反侦察 反监视 自检
[image] 关联	[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法 ；[image]反监视 ；[image]监控侦测 ；[image]物理监控（上岗） ；[image]暗中监视的迹象
[image] 创建时间	2025年2月21日
[image] **Description**	行动安全性

听说有些时候聚会吃顿饭都有便衣跟踪？但你不一定就有能力发现跟踪者，因为这是个技术活儿，具有较高的专业性。

- Table of Contents

你应该注意哪里？
静态监视：
移动监控：
如何发现监控
静态监视检测：
移动监控检测：
棘手的技巧……
监视检测路线（**SDR**）
说在最后

[image]

本文将介绍一些技术，以检测是否有人正在对您进行监视。在我们开

始之前，我想明确指出，我在这方面的知识和经验来自私营部门，而不是来自任何秘密的政府机构工作。我们将要讨论的原则和技术是可以全面有效的，尤其是在应付警务外包方面。

对于政府监控，您需要在对政权最有可能采取的措施做出较为充分的预测的基础上，针对性选择我们提供的方法。如何预测？如果您一直在关注本博客就能明白应该怎么做。就如中国人喜欢的俗语：知己知彼方百战不殆。只要您有心，就肯定明白这些工具的真正用途。

你应该注意哪里？

简短的回答是，这取决于您的位置，以及您是静态的还是移动的。

下面我们分头说。

[image]

激进社区用户请从这里进入：[image]物理监控（上岗）

静态监视：

如果你是静止的，那么对你的监视很可能也是静态的。

让我们来看看有可能找到你的两个最可能的静态位置—你的家和你的工作场所。这些非常重要，因为如果你已经被作为特定目标了，那么可以推测，监视者能够定期甚至经常地在这两个地方找到你。

为了弄清楚监视的位置，你要做的就是让自己置身于一个潜在的监视者的角度，并试图弄清楚你的位置，以隐蔽地观察前门或通往你住所的车道，以及工作场所的主要入口或停车场入口。记得那句话吗？——像骇客一样思考。

不要只是理论化，你应该实际尝试在现场的感觉。有没有方便的咖啡馆、繁忙的十字路口、公共汽车站或火车站、公园或城市长椅等可以让您在很长一段时间内获得良好的位置和足够的掩护？如果是，那些可能是您想要缩小注意力的位置，而不是试图覆盖整个区域。

您还需要注意停放在可能为监视者提供良好视野的地方的车辆（如果该区域没有如上所述的任何良好的有利位置，这一点就尤其重要）。如果存在这样的有利位置，并被流浪汉或者移动摊点所占据，那么监视者很有可能伪装为流浪汉或摊主，也就是说，第一步应该重点关注的是位置而不是看起来是否可疑的人。

一个训练有素的监视者要做的第一件事就是，把自己的真实身份融入周边环境中。还记得 BACK [image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A 中介绍过的观察法吗？在这里它反着用：如果你不希望被人发现或关注，那么你就应该表现得与周边和谐一致，在多方面的细节上。

这属于较高水平的敌对监视，也许你在现实中遇不到这么高的水平，但如果你能以高水平的基础掌握这些观察技能，你将可以应对一切水平模式的敌对监视。

移动监控：

在进行移动监控时，事情变得有点棘手，因为监视者也可能需要移动。

在运动状态下，监视人员通常希望在目标后面的某个地方，并且可能在后侧面，而不是直线（那样有点傻。或者说如果你只关注直线后方，也有可能会傻）。

当目标在典型的城市人行道上向前移动时，我们可以想象潜在的监视区域范围：一个是在目标后面，一个在后面但在街道的另一侧，当它向前移动时将被“拖”到目标后面。

关于移动监控最具挑战性的事之一是当目标不可避免地停止时（无论是短时间还是较长时间），监视者需要做的事情。这是因为目标从移动切换到静态，然后可能再次返回移动状态，这些过渡点对监视者来说是真正的挑战—因此也为您提供了探测好机会—因为监视者必须快速弄清楚如何继续跟踪他们的目标，而不会出现任何令人惊讶的、混乱或紧张的迹象。

如何发现监控

主要通过注意与目标的相关性来检测监视。因为在这种情况下，你自己是目标，所以挑战在于发现某人是否与你有关，即使他们故意试图从你身后或在你视野之外的角度来监视你。

如果你不想透露正在寻找监视这一事实，就不得不想方设法简要地浏览上述监视有利位置（静态和移动监视点）。简单说就是，你能看到有人在看你，在你移动和停止时，或者只是在不同的地方在一段时间内以某种方式多次出现“碰巧”。

听起来有点棘手，因为大多数可能下处于潜在有利位置或在街上走在你身后的人都没有试图监视你。我不想把你变成疑神疑鬼的人，但是你应该知道自己什么时候需要做这样的警惕。

要知道，监视人员与其他任何人的不同之处在于，他们有意地试图观察你在哪里以及你去哪里。因此，监视人员肯定会展示出与您的积极关联—特别是在时间和距离上—这是最重要的指标，可以将监视人员与周围的其他人区分开来。

发现这些相关性并不总是很容易的，但通过练习，肯定能做得更好。

以下技术旨在检测一些经典的监测指标，忘掉那些关于“可疑人”的典型特征，有些书描述的东西完全是错的。请记住，如果被高级情报部门监视、或者如果您正在被一个协调一致的操作团队来进行监视，光靠这些可能不够。

好消息是，您可以随时随地练习这些技巧—逐渐变得更好，更精细地应用它们。逐渐趋向能应付更高级的和团体协作的监视状态。

静态监视检测：

- 当您在家、工作地点、餐厅、酒吧等地时，试图找到来自*外面*的视角（通过窗户、入口等）。试着看看你是否可以在有利视角的位置找到任何人，或者只是在外面徘徊的人，看看谁会密切关注你可能会使用的入口/出口。

- 当您出来时，使用自然的转头和周边视觉来查看是否有人注意到您的退出，并正在准备从静态转移到移动状态—从而与您自己的转换相关联。

移动监控检测：

1. 当你向前迈进时，试着找到创造性的方法，在你身后的区域、但在街道的另一侧，瞥一眼。这样做的一个好方法是定期侧视，并使用周边视觉来看待你身后（商店橱窗是个好东西哦）。你需要隐藏自己这种观察动作，让自己看起来是对身边的东西感兴趣，而不是身后的东西，看看华丽的汽车或走过身边的有吸引力的人，等等）。尽量不要夸大这些动作，保持自然。您需要的只是极短的一个目光，即便发现了跟踪者也要当作没发现一样。这很重要。

1. 使用人行横道，红绿灯或其他常见的可以短暂停留的理由，来自然环顾四周，从而获得更好的外围视图，了解您背后的情况。

1. 找到合理的原因，穿过你正在走的街道的另一边。你将要做的 90 度转弯可以将你身后的区域尽收眼底，当过马路时，你可以更轻松巧妙地覆盖周边视野。

1. 使用短暂停留（浏览商店橱窗、等待步行信号、检查手机等），试着注意你身后的人是否也突然从移动过渡到静止（从而与你的动作相关）。

1. 使用更长时间的停靠点（走进商店、咖啡馆等）快速查看前窗或门，看看是否有人从移动过渡到静态，是不是有人正在观察您刚走进去的方向，或者有人开始走近你。然后重复上面静态监视检测部分中提到的两个步骤。

1. 使用微小的假动作来判断您是否可能暴露。保持简单和微妙。尝试执行以下操作：

- 走过一个带窗户的商店，然后停下来，转身回到商店。

- 当你坐在咖啡馆里，起身时（好像你准备离开）收拾你的东西，然后去柜台点东西，或者去洗手间，然后回到你的桌子或另一张桌子。

- 当然，您可以执行许多其他此类操作，并且所有这些操作的重点是：做一些监视者难以预料的动作，因此更有可能导致技能较低的监管者犯下经典的错误。这些错误通常会出现引起紧张混乱、双重攻击、从静态到移动的不自然的转变，以及不自然地重新回到静态等等的形式，这将很容易帮助你找到存在相关性的机会。

记住监视者总是与他们的目标相关联，问题在于他们能够隐藏它的程度，这些行动可以决定相关性能被发觉的程度。老练的间谍是很难被发现的，但一般情况下大家遇不到摩萨德那种高手。

棘手的技巧……

许多人喜欢好莱坞式的使用反光表面、窥视孔或小工具的想法。我不是那种东西的粉丝。并不是说通过观察反光表面来发现身后的人是不可能的，但如果过度依赖这种策略，你可能不会做得好。现在我们的

目标是提升你不需要借助什么东西就能在现实中操作的能力，而不是拍电影为了看起来精致。

此外，盯着窗户（或者更确切地说是它反射的东西）或使用笔记本电脑或手机的黑屏来反映你背后的东西，比你想象中要更明显。甚至一些老掉牙的套路也是有效的，例如故意掉东西以便在拾起时能环顾四周，或者停下来绑鞋带。别笑，这些都是有用的。

监视检测路线（SDR）

SDR 是您可以提前计划的预定路线，旨在巧妙地暴露敌对监视。它基本上将所有上述策略整合到一个计划的序列中，仔细选择一条路线，引诱监视人员跟随你。

典型的路线需要从您希望找到的逻辑位置开始（您的工作场所就很好）。路线不应该是您通常采用的路线，因为如果监视人员已经明确知道您要去哪，他们就不需要跟随你了（他们可以在那里等你）。相反，不要让这条路线太奇怪，因为监视人员可能不会想要跟随你，或者更糟糕的是，可能会怀疑这是一个陷阱。

确保路线中有短暂停留和长停留（您已经知道要查找什么了，以及从哪里查看）。如果存在监视，这将增加隐蔽检测监视的可能性。

[image]

激进社区用户请从这里进入：[image]反监视

说在最后

另外简单说几句外观问题。外观在反侦察术语中被称为“封面”，包括从衣着到神态到言谈举止，都要高度符合你希望自己伪装成的那个封面的特征。绝不能够你的衣着看起来像个乞丐、你的自我介绍是“无家可归的可怜人”，而你的神态警觉地瞄向四方暗藏杀机……那样的

话你就演砸了。

这是一件非常微妙的事，需要强烈的意识来控制它。绝大多数情况下负责这种隐蔽行动的监视方都是便衣，而不是伪装成乞丐、小贩什么的。因为没有那个必要，除非是集体行动的监视。

要注意，并不存在绝对意义上的“便衣”，人们通常说的便衣只是代表“此人没穿制服”。此人的便装也会带有浓厚的个性特征，有可能他自己都意识不到这些。但很简单你可以判断。每个人的衣橱里都有几件根本不会去穿的衣服，你感觉它们不适合你（鬼知道当初为什么会买来）或者说不适合你的平常状态，不过请注意，那几件衣服就是你伪装自己的绝佳道具 —— 它们不带有你最容易被暴露的个性特征。

不论你是监视者，还是躲避监视的目标人，这些细节都是特别重要而需要掌握的。我们的主题是为后者服务，那么当你排查监视者时，请注意这些下意识中难以隐藏的东西。

也就是说，经过练习你完全可以通过一个人的穿着细节、言谈举止来挖出其可能的真实身份信息。要知道，被派来实施这类秘密行动的人很可能都有军事或警务背景，他们经历过很多相关的训练，这些训练完全可以塑造其个性和品味，普通人都有这种经验，当过兵的人看起来不一样，没错你的直觉就是对的。

并不是说看起来膀大腰圆、目光炯炯、穿着战术靴、使用坚固耐磨的手机壳和防水手表的人都是可疑人，绝对不是，上述所有观察点应该被结合起来使用。充分调用你的直觉，它往往有很高的价值。

如果您对反侦查感兴趣，我们在未来将会介绍更多实际操作的技巧，包括在被捆绑束缚后脱身的方法、以及能帮助躲避灾难的防身之术。

好啦，记得常练习哦，包括我们以前介绍过的观察人的技巧等，当你熟练之后就能游刃有余了。今后我们还会继续介绍相关技巧。反侦察是一门复杂且专业性很高的技术。

[image]
[image]

暗中监视的迹象

[image] 关键词	反侦察 反监视 威胁识别 监测
[image] 关联	[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ ；[image]物理监控（上岗）；👀大规模监视 ；[image]隐蔽的监视设备 ；[image]隐蔽性地突袭住所
[image] 创建时间	2025年2月22日
[image] **Description**	技术直觉；行动安全性

您知道政府正在如何监视您吗？您不需要是什么特殊的人物，就如我一样普通，也同样”享受”着这一系列监视。您应该知道怎样识别它们的存在。

- Table of Contents

  1. 如果你有一部“智能”电视
  2. 您尚未更新设备
  3. 你在机场被标记了
  4. 你正在分享你的cookies
  5. 你打开了可疑的电子邮件
  6. 你的名字和政府监视黑名单上的某个人姓名相同
  7. 你在自己的车子上找到了一个跟踪器
  8. 您的数据使用率高于您实际使用的数据
  9. 一辆没有任何标志的面包车停在你家门外
  10. 摄像头上的指示灯亮起—即使您没有使用它
  11. 在通话期间，您听到了奇怪的声音
  12. 家里似乎有些不对劲
  13. 周围的人
  14. 他们如何跟踪你的电子邮件

15. 他们如何跟踪你的浏览
16. 你在开车的时候他们如何监视你
17. 你注册会员卡和信用卡时他们如何监视你
18. 当你走在大街上他们如何监视你

[image]

技术正在飞速发展，政府的权力也是一样。如今几乎每个人都知道政府正在监视自己，但其中仍有很多人把这想得太简单了，就如公民社会组织 ACLU 所说：政府比你想象的要狡猾得多。

如何判断自己正在被监视？

本文列举一些值得注意的奇怪迹象、以及危险度比较高的情况。一旦您发现所处的环境与这些迹象相符，请尽快撤离，或想办法缓解。

1. 如果你有一部“智能”电视

几年前我不知道为什么会有人想要买这种东西回家，它是一个活间谍。可惜如今你已经几乎买不到普通电视了，因为市场生产非“智能”产品不赚钱。而且不止电视机，有可能很快，你将会买不到普通的门锁、买不到普通的吸尘器、甚至普通的灯泡……

你所有的所谓“智能”技术都很酷 —— 但它们不会给你的隐私带来任何好处。Wikileaks 文件中曾经最著名的部分就是揭示了中央情报局可以闯入三星智能电视。

受到这种工具感染的电视机被隐藏录制音频，一旦电视机完全切换回来，将通过互联网传送数据到间谍机构的计算机服务器。

截至2016年，中情局已经建立了 24 个 Android 的“零日”武库。其中一些据说是由中央情报局自己开发的，其他一些据称是从英国的 GCHQ 机构以及 NSA 和未命名的第三方获得的。

请注意，您正处于无国界零日战争的鼎盛时代……

[image]

返回：https://iyouport.substack.com/p/d09?utm_source=publication-search

返回：https://iyouport.substack.com/p/e3b?utm_source=publication-search

中央情报局中还有一个专门单位其工作就是瞄准 iPhone 和 iPad，允许该机构看到目标对象的地理位置、激活他们的设备的摄像头和麦克风，并阅读文字通信。该部门还利用 GCHQ，NSA 和 FBI 获得的进一步 iOS “零日漏洞”。

没有哪个政府不想这样做，除非他们不能。尤其，别忘了， 中国当局目前是全球三大零日巨头之一。

所以，如果你家有这类“智能设备”，请在家里时小心说话。

2. 您尚未更新设备

不论如何，你必须依照最基本的网络卫生。

防止安全漏洞的最佳方法之一就是：保持设备更新。过时的软件更容易受到损害，监视者很乐意首先盯着那些懒人（可能因为0-day太贵）。

[image]

如果您已经是敏感人士，非常建议从这里开始：[image]数字技术限制和最佳实践

3. 你在机场被标记了

你可能会在机场被标记一次或两次，但请注意这是否经常发生。HowStuffWorks 解释说，如果你在机场多次被拦下，这就是一个标志，你的名字无论如何都在政府观察名单上。

Mental Floss 指出，现在已经有一些人由于有争议的社交媒体帖子而无法登机。虽然人们不能因“不可靠或不可信”的信息被列入黑名单，但是，社交媒体帖子肯定不会被监视者忽视。

4. 你正在分享你的cookies

存储在浏览器中的微小数据都可跟踪您一切的在线活动。这些 cookie 可以保留从您的密码到您想要网购的所有东西。Cookies 被放入一个巨大的数据库，公司可以在这里找出你的离线身份、并出售这些信息。

赫芬顿邮报解释说：“有两个主要群体可以访问这些数据：政府（包括国家安全局和当地警察局）、以及私营部门（即：广告业）。”

再一次，没有哪个国家不会这样做。

5. 你打开了可疑的电子邮件

我们都收到了可疑的电子邮件。问题是你打开了吗？只需单击一下，即可将发件人引入到您的设备上。我们在社交工程攻击演示中介绍过这种跟踪。

无论是政府老大哥还是垃圾邮件发送者，都会威胁您的个人隐私，您首先要做的是删除那种电子邮件而不要打开它。无论如何都不要回复那种电子邮件。如果攻击者确认您的帐户处于有效状态，就会引发进一步的间谍活动。

6. 你的名字和政府监视黑名单上的某个人姓名相同

即使你没有做任何让自己进入政府监视黑名单的事，也可能那个名单上有与你同名的人。如果这样的话你也可能会麻烦。不用想着改名字，因为你根本不知道那个名单上都有什么名字。

HowStuffWorks 在2004年的报告中写道，一位名叫 John Lewis 的人在政府监视名单上。这是个特别普通的名字。在接下来的几年里，由于名字相同，每一个叫 John Lewis 的人登机都会遇阻。

检查您的姓名是否在财政部公布的特别指定国民和被封锁人员名单上，以确保没有不受欢迎的未来意外（包括查水表）。

7. 你在自己的车子上找到了一个跟踪器

政府可以密切关注的不仅仅是您的技术工具。很多情况下跟踪器通常隐藏在汽车的底盘中。它很小，以至于很多时候难以发觉，它们也可以安装在轮舱或排气系统中，因此有人可以随时跟踪您的汽车位置。

[image]

关联相关页面：[image]监视器排查

如果您觉得自己被跟踪了，或者行程比较敏感，在上路之前请仔细检查您的车子，特别是在较小的缝隙中。

你要提防的不只有警察和间谍，因为如今任何人都可以在线购买到这种微型跟踪器。很便宜。

8. 您的数据使用率高于您实际使用的数据

您是专有Wi-Fi 的用户，但您的数据正在逐渐增加。这是为什么？“今日美国”报道，可能是因为国家安全局可能正在侦察您的行踪。而且当地警方也开始使用相同的做法。

因为数据量上升可能来自间谍软件，它可以追踪您的日常生活的一切。攻击者也可以使用此技术窃取您的个人信息。

9. 一辆没有任何标志的面包车停在你家门外

不，这可不是间谍电影里的俗气道具。政府确实在使用无标志的车辆进行监视。

[image]

关联相关页面： [image]隐蔽监视

不是每辆停在你家外面的面包车都值得关注，但一些关键指标可能意味着它是一辆监视车。

寻找那些带有色窗户的无标志货车，这些车辆停放数天，没有任何人进入或离开车子的迹象。

[image]

更多相关内容可参加S06：[image]S06反侦基础课 - 总章节：敌对环境中的生存训练，和特工战斗法

10. 摄像头上的指示灯亮起—即使您没有使用它

指示灯亮起时意味着您的网络摄像头已开启。如果您的网络摄像头指示灯即使在未使用时也会亮起，请不要认为它只是故障。可能是条子正通过你的相机看着你。

这里有一些更可怕的东西：每日邮报在线报道，政府有技术可以触发您的网络摄像头，甚至不会让灯亮起来。也就是说，你可能会在没有任何意识的情况下被窥探。

如果您担心这点，那就不使用网络摄像头。或者用一块不透明胶带盖住它。覆盖镜头可以防止任何潜在的间谍看到任何东西，但请记住你的麦克风可能仍然会被远程打开！

[image]

如果您已经是敏感人士，请注意这些原则：[image]户外无设备对话

11. 在通话期间，您听到了奇怪的声音

是的，这意味着窃听发生了。如果您在手机上听到噪音，例如点击、弹出、刮擦或其他奇怪的声响，那么有人可能正在监听您的对话。

另外，请注意手机在不使用时产生的噪音，这是另一个标志，意味着有人正在搞乱你的线路。

[image]

关联相关页面：👂窃听 ；[image]隐蔽的监视设备

12. 家里似乎有些不对劲

你应该最熟悉自己家里的布局应该是什么样的了，尤其是一些小的细节。你真的应该牢记这些小细节。因为，Business Insider 指出，警方可以在没有告诉您的情况下、在没有任何保证的情况下，在私人财产上安装隐藏的监控摄像头。

这并不意味着政府会选择偷偷潜入任何人的家，但是，如果他们认为你对政权b“构成威胁”，你可能会发现你的整个家都被窃听了。

[image]

关联相关页面：[image]隐蔽性地突袭住所

13. 周围的人

NPR 采访了联邦调查局特工，发现他们是融入人群的专家。这些特工表示，他们已准备好了为所有类型的活动搭配的衣物，能够非常好地融入他们正在监视的人群中—— 参加大型群体事件时尤其需要注意这点。

[image]

关联相关页面：[image]匿名着装

如果你是单一目标，当你被跟踪时，通常会有整个团队围绕着你，尽管你可能不会注意到。现在您应该知道：如果认为自己被跟踪了，那么记住可疑的面孔而不是衣服是很重要的，因为衣服和头发随时可以换。

14. 他们如何跟踪你的电子邮件

你是否曾经在电子邮件中讨论过某个产品或服务，然后在事后看到了一堆相关的广告？很简单，你的邮件被监视了。

你不应该对此感到惊讶，因为雅虎和谷歌都有权扫描你的电子邮件，为你提供更具针对性的广告。我们一直强调不要使用Gmail，这是最主要的原因之一。

并且，您的电子邮件服务商可能不是唯一一个阅读这些内容的人。 政府间谍也可以随时查看您保存或共享的任何电子邮件、图片、文件和社交媒体帖子。

[image]

关联相关页面：[image]服务提供商协助调查

15. 他们如何跟踪你的浏览

你可能已经允许网站在没有意识到的情况下使用 cookie 来跟踪你，它会记住您的密码和您查看的项目，所以在某种程度上，它们可以会让人感觉很方便。但是，你必须禁用它们。这些cookie 中的信息会出售给你都不知道是谁的人以了解关于您的更多信息。

政府也可以访问这些信息。虽然广告业和私营部门可以比政府收集更多关于你的信息—而且他们也完全会从中获得巨额利润。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

16. 你在开车的时候他们如何监视你

即使您在没有带手机的情况下离开家，他们也有办法密切监视您。

ACLU 指出警车和道路标志都可以使用自动车牌阅读器作为监视。扫描您的车牌号码、日期、时间和地点。然后，这些信息会被汇集到当局的大型数据库中。

有些信息会被保存多年—甚至永远保存。如果你出行的路线是一个比较敏感的地点 ...不要使用任何私人车辆。

[image]

关联相关自卫措施：[image]反监视

17. 你注册会员卡和信用卡时他们如何监视你

每个人都喜欢优惠价，这就是会员卡如此受欢迎的原因。你可能已经注册了几个—— 而且它们可能为你省钱。但是，您可能没有意识到某些会员卡、信用卡和类似东西很容易监视你。

使用这些信用卡和会员卡可以存储任何关于您购买行为的数据，并且会出售这些数据以及您在线活动的统计数据，以便向广告客户提供有关您的更多信息。

当然，法律还可以要求访问您的信用卡历史记录。

[image]

关联相关自卫措施：[image]匿名购买

18. 当你走在大街上他们如何监视你

国安局花了数百万美元购买高科技摄像机，为了在你走在街上时监控你。2012年，ACLU 报告仅在芝加哥就有1万部公共和私人拥有的摄像机。如果您在中国，当地的城市可能会有很多。

并且请记住，如果你居住的楼层比较低的话，这些玩意可以通过窗口看到你家里。所以，请记得随时拉上窗帘。

[image]
[image]

如何安全地留住证据：给真相的记录者一些技术技巧建议

[image] 关键词	个人 反追踪 反间谍 威胁模型 工具 独立调查 自卫
[image] 关联	[image]给公民记录者的技巧指南；[image]公民取证技巧：如何留住真相？；[image]当你手握真相：最基本的防护知识
[image] 创建时间	2025年3月1日 9:00 (GMT+8)
[image] **Description**	行动安全性

任何时候，拿出充分证据都是取得胜利的重要基础。中国有很多问题无从解决是在于证据的缺失，活动家们的技术能力不够、对证据的保存不很用心，并且一直在遭到当局的骚扰和审查。这就是为什么技术普及是至关重要的：技术不仅能保护铁证不会丢失，并且能保护记录者和其中涉及到的所有人的人身安全。

- Table of Contents
评估您的风险
学习如何保护自己和他人

[image]

如果你正在记录侵犯人权的行为、社会敏感问题、政府阴暗面，互联网可以帮助将真相传播到前所未有的广度让人们知晓，同时也可能会让你入狱。

无论你是保护环境的活动家、记录系统性国家暴力的公民记者、还是

驻扎冲突地区的独立调查人士，都要重点考虑数字记录和传输的安全问题，这不仅仅是为了你自己。

如果您无法妥善保护视频、照片和通信记录，那么您与之通信或传输文档的每一个人都将面临风险。只有更好的安全性才能更好地工作。

在中国，普通人也面临着极其严重的政府监视和间谍行为，安全知识、威胁警报和技术援助对中国社会来说尤其重要。然而很多人并没有重视起证据保护的环节，抓不住重点的拍摄记录反而令当局掌握了辩解的借口；被查抄的资料导致记录者和相关人等被逮捕、真相被掩盖；最终只有极少的证词而没有可靠的资料，很难平冤。

最初，数字威胁一直被认为是压倒性的，许多人认为需要特殊的技术专业知识才能理解和减轻所面临的安全威胁。中国社会似乎至今如此。这也是为什么隐私保护知识的传播非常困难。但这是一个错误的观念，虽然可以理解。

事实上，提高您的数字安全性只是意味着需要弄清楚您自己所面临的风险是什么，并由此判断您愿意学习哪些工具和技术来保护自己和周围的人。

安全培训师称此流程为风险评估或威胁建模。这听起来似乎有点复杂，但有如今许多组织都有在线创建资源，可以帮助您评估和满足您的数字安全需求。

本文列出了一些类似的指南，以及它们可以教给您的内容。

[image]

激进社区用户请从这里进入：[image]数字技术限制和最佳实践

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

评估您的风险

要得到更好的安全性的第一步是威胁建模或风险评估。这只需要问自己以下五个问题。考虑拿出纸笔，并可以和与您密切合作的人一起讨论这些问题，因为安全是一项集体的努力，一个人的安全可能无法解决整体问题：

- 我需要保护什么？
- 我需要防御的是谁？
- 他们想要多少信息，以及获取信息有多容易？
- 如果他们得到我要保护的东西会发生什么？
- 我愿意做些什么来阻止这种情况发生？

就这么简单。让我们使用一个具体的例子以便更详细地看下这些问题。

也许你拍摄了一名警察殴打抗议者的视频，这时候您就非常有必要保护您所创建的材料，因为当局会想尽一切办法销毁它，甚至将您逮捕。

不仅需要保护收集的数据不落入坏人之手，您可能还需要保护抗议者的真实身份。为了您自己的安全，您可能需要隐藏您拍摄了事件这一事实。总之需要保护所有这一切不受警察的影响。但也许您还需要将更多信息隐藏起来，例如，您的工作地点、真实姓名等，因为您可能因为“激进”而被解雇。这只是需要保护的大量案例之一，你必须仔细考虑自己的情况。

一旦你弄清了需要保护什么以及防御什么人，接下来就会想到实际的风险是什么。也许您已经知道，警察经常会抢走人们的手机和电脑，他们对拍摄记录非常生气。而且你不知道他们有什么技术，但你需要怀疑他们可以通过你的手机了解到关键信息。

[image]

返回：[image]设备好像被黑了怎么办？ - 数字急救包

然后，如果您的安全性受到损害，您必须考虑后果，以及您为避免这些后果而愿意采取的措施。例如，警察抢走你的拍摄资料的后果可能只是你无法再公开这些真相了，但如果他们对被拍摄感到非常愤怒，可能会导致你最终受到警察的骚扰和威胁。也许这名遭到严重殴打的抗议者被反咬为“打警察”（这种事经常发生），并且由于你丢失了自己拍摄到的视频真相，这些指控就不会被取消。在这些情况下，您自己和您涉及的人的生命都可能处于危险之中。

最后，使用这些信息，您可以决定愿意采用哪些工具以及愿意改变哪些习惯性做法，以避免这种后果。例如，在手机上启用加密是一个简单的步骤，可能会使警方更难获取您的数据。也许你非常关心你拍摄的人并且不希望他们的身份被公开 — 他们所面临的报复风险可能非常大。在这种情况下，您可以考虑下载和使用 **ObscuraCam** 或 **YouTube Blur Tool** 等技术来删除视频的可识别部分。这可能比开启加密要稍微复杂一些，但它可以挽救一个人的生命。

学习如何保护自己和他人

任何时候证据都很重要。政府的恶行最怕被揭发和公之于众，中国当局称其为“负面消息”而被禁止传播，因为那是他们的罪证。

- 肯尼亚公民组织拍摄了几个小时的公民证词和现场录像，关于他们的房屋被政府强行拆除的证据，最终非洲最高地区法院作出判决，将土地还给人民。如果没有这些证据，就无法获得这样的裁决；

- 一名美国公民拍摄了警察打人的视频，然而她被警察诬告“袭警”，在她被强行居留的时候，警方删除了她设备上储存的视频，也就是警察打人的证据。但警察没想到她首先将视频上传

到"云端"了，最终她拿出证据证明了自己的清白；

- 危地马拉的活动家拍摄了政府暴行的证据，记录了当地人民抗争的过程，作为人权纪录的铁证……

WITNESS Library 提供各种各样的资源，使用超过十五种语言介绍公民反抗的技术技巧；两个最全面的在线指南是 EFF 的" 监视自卫 "（SSD）和 Tactical Tech and Frontline Defender 的" 安全盒"，"这两个站点都准确表明了他们上次更新的时间，这很重要，因为反抗技巧出现后，当局的反制技术就会随后出现，数字安全资源可能会过时；SSD 提供针对特定情况的指南（例如"跨越美国边境时需要考虑的事项"），有关如何使用特定工具的详细教程，以及针对特定人员（如记者或 LGBTQ 青年）的建议工具列表。有英语，法语，西班牙语，俄语，土耳其语，越南语，葡萄牙语，泰语， 阿拉伯语，阿姆哈拉语和乌尔都语；Security-in-a-Box 有十五种语言的版本，还有一个全面的工具和策略列表，以及一个侧重于特定社区的部分，例如中东和北非的 LGBTI 社区。

其他有用的资源包括：

- Tactical Tech 的"Z en and the art of making tech work for you "指南，专注于"女性和跨性别活动家、人权维护者和技术专家"，并拥有一些独特的资源，如"在线创建和管理身份"。它尚未完成，但仍然非常有用。有英语和西班牙语版本；

- Rapid Response Network 的数字急救包 "旨在为面临最常见类型的数字威胁的人提供初步支持。"当您已经受到入侵时，该套件特别有用，因为它会给您具体的指导；

- Crash Override Network 为避免成为在线滥用目标的人提供网络安全资源，包括 Doxing 预防指南（doxing 是您的电话号码、法定姓名和家庭住址等信息的公开）。他们的指南有一些针对美国特定的信息，但他们有很多信息对任何人都有用；

- 自由软件基金会的"Email Self-defense "，在十五种语言版本，

是保护您的电子邮件的好资源。

获得这种知识的能力意味着您争取人权的斗争是否能成功。

[image]
[image]

给公民记录者的技巧指南

[image] 关键词	独立调查
[image] 关联	[image]如何安全地留住证据：给真相的记录者一些技术技巧建议；[image]公民取证技巧：如何留住真相？；[image]当你手握真相：最基本的防护知识
[image] 创建时间	2025年3月2日 10:00 (GMT+8)
[image] **Description**	行动安全性

本指南应该适合任何突发事件中的公民行动。

- Table of Contents

  在疫情期间的记录权
  一般安全原则
  如果您要分享这些视频记录
  记录防疫期间的过度权力使用
  要注意您的拍摄中需要包含必要的证据细节：
  拍摄人权自述视频
  提示：
  记录远程视频或音频采访
  尽可能不要分享错误的信息
  分享前需要检查：
  最后

[image]

拍摄和分享涉及人权的事件记录，可以揭露不公正现象、聚焦鲜为人知的故事、尤其是动员抵抗运动，以令肇事者和当权者负责。

但如果平常情况下追究人权问题的责任是危险的，那么在冠状病毒大流行的情况下更是如此。

[image]

在疫情期间的记录权

“记录权” 指的是：能够拿起相机或手机拍摄警察或军事人员的行为，而不会遭受报复的权利。

也包括行使这项权利所需要的主动性、承诺、态度和勇气，组织团体也正在努力实现这一目标。

记录权通常与公共场合相关联 —— 在世界各地的抗议活动中、在贫民窟和郊区、集中营和审讯室，以及任何发生侵犯人权行为的地方。

要明确这点，“记录权” 不仅限于街上。实际上，即使如今许多人由于 **COVID-19** 而被迫限制活动，行使这项权利也比以往任何时候都更加重要。

如果不是勇敢的医护人员制作的视频，人们不会理解这场危机的影响的全部方面，尤其是糟糕的政策对弱势群体造成的不成比例沉重代价。

全世界的人们已经看到大流行被用作创建和加强专制政府和政策的借口，不仅包括众多专制国家，也包括美国那样的所谓民主国家、以及匈牙利那样的欧盟成员。 BACK https://iyouport.substack.com/p/lr-covid-1984-?utm_source=publication-search

全世界的警察和军事部门也都在实施封锁措施。他们没有以公平的方式这样做，更不用说遵循国际人权法所要求的必要和相称原则了。他们根本不尊重人权。

当前急需将这一切记录在案，以便可以声讨权利和追究责任。已经有很多案例被记录，例如南非的强迫迁离、美国监狱和拘留中心的不人道状况、以及巴西无家可归者的危险状况。

法律观念和社会正义观念都很重要：毕竟，如果政府不尊重法律赋予公民的“权利”，法律的“权利”就不再重要，就没有任何法律能够保护社区为行使这项权利而采取的勇气、态度和主动性。

一般安全原则

如果您想行使自己的记录权，请记住以下几点：

1、您可以突破隔离规定以拍摄记录，但这不是被建议的。请务必注意安全，并请记住，如果视频表明您“没有正当理由”而突破隔离，那么当权者可以将视频本身用作证据证明您违反了法律。

2、如果您在街上拍摄并在他人可以看到您的地方拍摄，则无论记录权是否得到法律承认，都请与他人保持足够距离。至少可以确保他人在没有警告的情况下抢走您的相机或手机变得更加困难。

请记住，记录警察暴行为的人经常面临报复。这在任何国家都是如此。

3、如果警察阻止您拍摄、命令您退后，您可以向后退几步，然后大声说出来，以便在录像中能听到“我正在退后，警官”。

4、拍摄时，您可能需要设置自动备份。这样，即使您的手机被扣押，您也不会丢失文档。

但是请记住，备份到云可能会使数据容易被警察拿到。

[image]

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

5、直播是一种强大的工具，但是很危险。直播时您无法编辑视频以模糊受害人的面孔。所以您需要一些技巧。

6、记录权的法律状态因国家而异。这里有一个记录权地图，可能包含有关您所在国家/地区的相关法律信息。

7、拍摄完成后请务必注意发布问题。请记住，在有些国家拍摄或随后分发可能是非法的。即使拍摄和发布都是合法的，您仍然可能会遭受报复。

最后，即使您本人的匿名状态很好，在您的视频中出现的人也可能会遭受报复。您需要考虑这点，并有一个明确的道德准则 —— 与您所在团队的所有人共同遵守。

8、秘密拍摄在许多地方都是非法的，但对于记录人权侵犯来说，它可能是您唯一的选择。美国也一样。您所在国家/地区的类似法律也可能涵盖对秘密拍摄的规定。您需要先了解清楚。

[image]

如果您要分享这些视频记录

在您分享视频记录之前请问自己以下问题：

- 视频中有可识别出身份的人吗？他们是什么形象？那些人知道自己正在被拍摄吗？如果被广大观众看到，他们在镜头中的出现会对他们自己或他们的社区产生怎样的影响？

- 拍摄视频的意图是什么？是为了记录侵权行为而拍摄的吗？它是否煽动了仇恨或恐惧、或美化了暴力？

- 谁是目标受众？该视频是准备被广泛地传播收看，还是为了特定范围内的观众群体所拍摄的？

- 视频中是否包含令人震惊的图像？这样的图像是没什么必要的还是对记录特定事件至关重要？您如何在观众观看之前警告他们其中包含此细节？

- 您确定视频是真实的吗？视频是否可能被操纵或被误解以至于形成误导？

- 分享该视频的目的和受众范围是什么？分享视频的潜在利益是否超过潜在风险？

作为记录者，您需要在您的组织内创建准则，以确定如何以道德的方式捕捉和分享视频。

以下是一些需要准备好答案的问题：

- 您什么时候可以保护被拍摄者的隐私和匿名性？您会帮助遮盖虐待受害者的面孔吗？（儿童？维权人士？）

- 您将如何公开分享视频片段？链接到原始在线视频吗？将视频嵌入到您的在线内容中吗？还是在自己的频道上创建新版本？

- 您将如何向观众指示素材的来源和背景？

- 如果还没有确定视频的真实性，那么您如何决定是否使用它、以及如何向观众指出其不确定性？

记录防疫期间的过度权力使用

政府可以依法限制行动，但是命令和行动必须必要且相称。防疫不是过度使用武力、缺乏透明度、歧视或暴力针对边缘化社区的借口。

如果您发现当权者超出了权力边界，您应该记录下这些证据。

首先，了解您所在国家/地区有关记录和研究权利的规则，并分析它们在大流行等紧急状态下可能受到的影响。

[image]

要注意您的拍摄中需要包含必要的证据细节：

- 警察官员的人数、他们的位置、制服、武器、车辆、车牌、路障
- 被损害的平民财产
- 尽可能捕获时间、日期、以及任何有助于验证地理位置的参考元素
- 拍摄受害者相对于警察的位置。受害人举起双手向警察投降，但仍被枪杀致死，这一要点必须清晰被体现
- 保持每次拍摄间隔10秒钟；如果距离较远，请按远处的物体进行对焦
- 缩放会扭曲图像，避免这样做（或将照相机靠在坚固的表面上）
- 现场是否有其他摄像机（监视相机、警用摄制器材）把它们包含进去
- 富人区与贫困地区的警务对比：警察保持着规定中的距离吗？

戴着口罩吗？是否使用了致命武器？

拍摄人权自述视频

当全球关注的焦点被集中在政府主导的主流媒体叙事上时，活动家社区的故事可能会被压制和忽视，甚至更糟。

如果您想通过录制视频来讲述自己的故事，这里有一些如何使视频外观和声音达到最佳效果的提示。

提示：

- 开始拍摄时，请先至少等待5秒钟，然后再开始对着手机讲话，然后在结束录制之前再等待5秒钟。这将帮助您进行编辑；

- 将相机支撑在平稳的表面上（如果可以的话请使用三脚架）。Instagram 和 Snapchat 等许多应用程序都提供了 “hands-free” 选项，您无需按下按钮即可进行拍摄。您可以使用该应用来拍摄视频，然后将其下载到您的相机中。只要确保不将其公开发布到应用程序即可；

- 如果在室内拍摄，请坐在窗户附近，但要确保窗户/光线来自您的前方（手机/计算机的后方）。这将有助于在您的脸上提供良好的光线；

- 如果在室外拍摄，光线应该是很好的，但要确保周围环境不要太嘈杂；尽量避免在正午时间进行拍摄，因为那样会在您的脸上投射更多阴影；

- 将手机/相机放置在与您视线齐平或稍高的表面上，以使您看起来像在平视相机并直接与他人讲话。您可能需要一些支撑物以帮助将设备提升到合适的水平（垫一堆书就能做到）；

- 在拍摄时，最好在背景中有一定深度，而不是直接坐在墙边上；

- 如果可能的话，尝试找到一个安静的拍摄地点。躲避警笛和汽车鸣笛等外部背景噪音。还要提防内部噪音，例如儿童、鱼缸或空调等；

- 如果您无法进入安静的空间或没有带麦克风的耳机，则应将手机尽可能靠近脸部;

- 如果可能，请尝试添加有助于人们形象化地描述您的内容的素材。例如，如果您谈论的主题是食物短缺，那么杂货店的空架子或排长队的背景画面可能会有所帮助。您也许还可以使用免费的素材库。

记录远程视频或音频采访

被监禁的个人及其家人发布了有影响力和有效的视频证词，以展示监狱和拘留所中的虐待行为，记录这些证词很重要，以便更好地保护他们的权利并敦促当局放人。

基于与受影响社区和反抗运动合作的经验教训，美国的团队调整了指南，以帮助更多的人学习如何记录远程音频和视频采访以协助维护人权。

在唯一的通信方式可能是屏幕或手机的情况下，这些技巧将帮助您进行远程采访并选择可用于录制的工具。

[image]

尽可能不要分享错误的信息

冠状病毒大流行已经极大地改变了全球卫生状况、运输基础设施以及经济。同时，它也对信息领域产生了巨大影响，导致大量虚假的或误导性信息充斥互联网，被称为“信息流行病”。

在危机中，人们会很自然地希望通过与朋友或家人分享防疫提示来提供帮助。但是请记住，不正确的信息只会引起过度恐慌，并导致增加感染病毒的风险。

这里有一些技巧，可帮助您验证在线观看的图像和视频，并记住，任何时候如果有疑问，请在共享之前进行检查。

分享前需要检查：

1、您肯定已经知道，大多数错误信息都是通过对旧视频简单地添加新描述而产生的，这很容易做到，只需几秒钟，而且很容易骗人，尤其是在疫情的大环境下，人们倾向于宁信其有。

您可以做的最好的事之一就是放慢脚步：“暂停”一会儿，仔细思考一下。您如何确定图像或视频是真实的？如果不是，您的分享是否会让别人更加恐惧，或令更多人受到伤害？一旦您花了一些时间开始认真思考，接下来的一些技巧将有所帮助。

2、您可能并不总是知道一张图片或一个视频的来源，但如果您知道如何调查来源，将对验证内容有很大的帮助。

如果来源是社交媒体，检查发布者账户中的描述，并寻找位置标签。

该账户是最近才创建的吗？如果是，这可能是一个危险的信号（虽然不总是如此）。该账户的其他帖子与你看到的内容中的细节一致吗（例如，分享视频的人真的是军事官员、医生吗，如果他们没有认证身份）？他们真的住在他们声称内容来自的同一个城市或国家吗？如果不是，那就不是一手资源，他们也是分享者，并有可能搞错状况。

当发布者账户的详细信息与发布的内容不一致时，你应该警惕分享。

如果信息来源是一个聊天应用，可能信息会较少，但你仍然可以调查。如果信息是被转发的，你可以问问转发者是在哪里找到的？如果是在群里发布的，那么这个群是否有良好的信息来源记录，还是容易出现谣言？

这都是最基本应该做到的。

3、全世界的记者都在努力对战冠状病毒危机。这意味着重大事件不太可能没有在任何新闻来源中进行报道。例如，如果您看到一段视频声称 “坦克正在某某道路上制造路障”，请搜索是否可以在网上找到任何其他证据。

当然，并不是每个故事都会在新闻中被报道。但是，如果一个图像或视频声称了一个重大事件，而又没有其他报道的记录，那就要对其产生怀疑。

4、虽然图像或视频的焦点通常是发生在其中的故事，但是背景中的细节往往揭示了更多关于拍摄时间和地点的信息，并可能证明发布者的描述是否具有误导性。

例如，如果能看到店面，那么这些店面是否与视频发布者所声称的事发国家/地区的商店特征相符？路牌是否使用了正确的字体和图标？其中人们的衣着风格是否是所声称的那个地区的风格？季节相符吗？……

5、如果您有时间进行一些真正的调查，使用图像或视频搜索可以是一个很好的方法，看看一个视觉媒体是否曾经出现在网上的其他地方。

对于视频，Google Chrome浏览器的 InVid 插件提供了一个强大的视频搜索途径，可以与 Twitter、Facebook 和 YouTube 一起使用。

这些工具都不是万能的，但它们都是调查视觉媒体的一个很好的开始。

更多验证信息的工具和方法，见 https://start.me/w/49bjyg。

最后

本指南应该适合任何突发事件中的公民行动，而不只是流行病。

您可以使用该指南在您所在的社区作为公民培训的基本资料。您还可以添加更多能满足您所在地区特征的技术技巧细节。

感谢 WITNESS 团队的贡献，您可以在他们的专题 COVID19 Response Hub 上找到详细资料。

[image]
[image]

公民取证技巧：如何留住真相？

[image] 关键词	工具 独立调查
[image] 关联	[image]如何安全地留住证据：给真相的记录者一些技术技巧建议 ；[image]给公民记录者的技巧指南 ；[image]当你手握真相：最基本的防护知识
[image] 创建时间	2025年3月3日
[image] **Description**	行动安全性

这是一场持久战，能给公民的最强大的武器就是技术能力和技巧经验。

- Table of Contents

  律师需要的证明包括：
  第一部分
  What：可能的基于犯罪的证据
  who & how: 可能的联系性证据
  第一步：
  第二步 使用相机麦克风或笔和纸来记录以下内容的姓名和联系信息：
  第三步：
  第四步：书面文档
  关键：
  第二部分
  第一步
  第二步
  第三步：整理您的视频
  第四步：跟踪视频
  目标

标题
说明
关键说明
第四步：保存
第三部分：与可信赖的个人和组织共享
第一步
第二步：决定如何提供原始文件给您信任的盟友以确保不会被更改
第三步；提供补充信息
最后
捕捉：在现场拍摄、并可以为您的视频添加上下文
保存: 保持媒体的安全和有序

[image]

世界各地的公民都在使用视频来揭露政权的恶行。视频作为证据也越来越多地被用作调查的一部分和法律指南。视频是证据收集的一个非常重要的工具，因为它有希望永远存在。如今几乎每个人都有一部手机，可以在任何地方拍摄和制作视频，中国曾经有所谓的“围观改变什么”的说法，我们一直不同意这一说法，主要因为：中国的大多数“围观者”由于严重不专业无法成为记录者；缺乏与人权组织合作的经验而无法令资料发挥真正的作用；因此他们并没能推动“改变”。

让证据发挥作用不是一件很简单的事，和中国一样，刚果的人权律师和社会积极人士一直面临着证明和理解事件背景的挑战，他们通常很难收集可以直接指控犯罪的关键镜头。公民证人、活动家和非政府组织，是第一批面对诸如此类挑战的人 — 关于如何捕获关键信息。希望能让视频成为证据的具体方法，应该建议活动人士与律师合作，这样他们就会对应该拍摄哪些重点心里有数，以便通过媒体、议会、国际权利组织、委员会和法院伸张正义。

虽然公民拍摄的视频经常提供关于发生的事情和可能性负责人的有用线索，但其质量很少能通过需要在法庭上作为证据使用的更高标准。好消息是：通过略微练习和修改，公民和活动家冒着生命危险捕获的镜头就可以作为刑事和民事司法程序的证据。

本文的主旨就是提供给所有勇于伸张正义的人们一些技巧和技术方面的协助。

我们开始。

首先，确定要拍摄哪些影像，为了让某人或组织对犯罪行为负责，

律师需要的证明包括：

- 犯下了什么罪行;
- 谁犯下的罪行;
- 是如何犯罪的（即 自己动手、有组织有计划、还是买凶等）。

公民和活动家通常可以很好地捕捉犯罪行为的镜头，但要记录犯罪者是谁、以及他们是如何做到这一点的，要困难得多。调查人员和律师要花费大部分时间来证明后者，因此，虽然记录犯罪行为的录像很有价值，但制裁和问责也很重要。在存在大规模暴行和系统性侵犯人权行为的情况下尤其如此。

记录犯罪的执行或后果的视频被称为“基于犯罪的证据”。以下是几个可以作为基于犯罪的证据的镜头示例。

录像片段：

- 军队折磨和伤害平民;
- 推土机非法摧毁房屋，以及推土机离开现场后造成的损坏场面;
- 警方非法杀害嫌疑人，并销毁致死记录;
- 空袭结束后，记录医院遭受的轰炸和破坏状况;

- 军营中的儿童接受战争训练;
- 可证实非法钻探的钻机出现的具体地点...等等

关于应该捕捉“什么”，有点本能的意味，你看到一些错误现象正在发生，就可以将相机指向它并按下记录。人们都有道德心理，这就是为什么有大量基于犯罪的视频记录。但捕获“谁”、及“如何”的证据远不那么直观并难以做到，以下我们介绍一些能帮助你的技巧。

包含关于“谁”和“如何”的线索的录像片段通常被称为“联系性证据”，因为证据将犯罪者与犯罪行为“联系起来”了。虽然有可能无法使用视频直接确定究竟是谁犯了罪以及他们是如何做到的，但视频可以提供重要的线索，调查人员和律师可以与其他证据来源（如文件或证人证词）拼凑起来 — 找出谁应该承担责任，即使肇事者已经远离犯罪现场也要追究其责任。

有时“谁”和“如何”这样的信息很容易用视频捕获，例如，

- 一名士兵的正脸，他反复殴打平民;
- 推土机操作员在摧毁房屋时的脸孔特写;
- 导致嫌疑人死亡的官员的徽章编号和铭牌...等等

然而，有些时候也会比较难。以下是一些对取证来说形成挑战的状况：

- 视频无法向我们展示正在投掷炸弹的飞机的飞行员的身份，或指示飞行员向医院投掷炸弹的指挥官的身份;
- 我们可能会在训练营看到儿童兵，但可能看不到他们的训练员或指挥官;

- 我们不知道是谁下令将钻机非法放置在土著人土地上的，因为我们只能看到钻机

- 一些便衣流氓在使用暴力针对手无寸铁的平民，但我们不知道是谁指使他们这样做的

联系证据至关重要。作为当地的公民证人或人权活动家，您可以独特地收集联系证据。虽然拍摄联系证据并不难，但了解如何捕获它比捕获基于犯罪的镜头更复杂。

第一部分

What：可能的基于犯罪的证据

- 正在进行酷刑

- 死亡

- 受伤

- 被官员殴打的人

- 平民财产受损

- 文物被损坏

- 携带武器或参加军事活动的儿童

- 仇恨言论

who & how: 可能的联系性证据

- 警察部队阻止抗议者和/或部队调动
- 徽章编号和制服
- 护照或其他官方身份证件
- 公务车牌照
- 军事装备（包括序列号）
- 演讲者
- 检查站
- 被占用设施的外部
- 曾经被占用然后被遗弃的设施
- 通信设备 — 卫星天线、收音机等……

[image]

第一步：

- 记录日期，时间和位置
- 确保将相机或手机设置为正确的日期、时间和 GPS 位置
- 录制您的声音，解说日期、时间和地点

- 如果您需要匿名拍摄，请在一张纸上写下时间，日期和位置，然后将其放在相机前至少10秒钟

- 您还可以拍摄任何可以显示日期、时间和位置的内容，例如时钟、报纸的头版、路牌、地标或地理特征

第二步 使用相机麦克风或笔和纸来记录以下内容的姓名和联系信息：

- 被拍摄的人物;

- 拍摄者;

- 现场其他与主题事件有关系的人。

第三步：

拍摄的目的是让那些不在场的人能够看到发生的事件，并理解基本要点。所以在拍摄时，问问自己，“如果我将这段录像给不熟悉该位置的人观看，他们能否总结一下所发生的事情，并根据我视频中的信息绘制出精确的场景地图？”你希望能够被回答，“是的！”

所以，对你拍摄的内容保持清醒和有目的性是必须的。活动家经常捕捉发生了“什么”，但不总是能捕捉到“谁”和“如何”。考虑填写“收集计划”表单，以帮助您战略性地确定需要捕获的素材，以便让观众清楚地了解发生的事件。由于每种情况都不同，因此没有绝对的规则，但以下是关键的基本拍摄技术，有助于确保您的视频易于理解和提供有价值信息：

当然能连续拍摄整个场景最好。但是，如果事件太大、很复杂或危险，您可能需要采取分片段拍摄。在这种情况下，请尝试通过将相机指向您刚才停止拍摄时的相同位置，以继续录制每一个新片段，可方

便剪辑。换句话说：重叠镜头。

包括以下镜头：

- 一个非常缓慢的 360 度平移，提供上下文并显示场景背后所发生的事。
- 广泛建立镜头，提供易于理解的犯罪现场布局，并协助验证时间、日期和地点。
- 采取旁观者视角，以确定犯罪现场的证据、位置、以及一件证据与另一证据之间的关系。
- 特写镜头显示关键细节并识别现场人员。
- 如果可能，请从事件场景的多个侧面拍摄上面列出的镜头。
- 保持所有镜头**10**秒或更长时间。更改位置或放大或缩小时，请缓慢移动相机。避免快速或不稳定的动作。如果可能，请使用三脚架、独脚架甚至固定表面都可以，以便稳定相机。

第四步：书面文档

如果您无法向录制的视频本身添加基本信息，则应创建一个单独的文档，其中汇总了有关您的素材的关键信息。一定要这样做，即使这可能有些耗时，但提供全面的书面文档可以显著增加您的视频被用作证据的机会。

摘要信息（通常称为“摄像报告”）可以手写或在计算机上完成，并保存在带有视频的文件夹中。

摘要始终包括以下内容：

- 您撰写摘要的日期和时间;
- 拍摄视频的日期、时间和地点;
- 以下名称和联系信息：拍摄者; 正在被拍摄的人物; 现场其他与事发信息有关的人;
- 视频中所显示内容的简短实际摘要。禁止错误信息和夸大描绘;
- 任何安全信息或安全限定。

关键：

书面文件很重要！即使您在视频录制中包含了基本信息，单独的书面摘要也会有所帮助。这些额外的文档将使您的视频在公民和活动家每天捕获和共享的成千上万个视频中脱颖而出，它将帮助人权研究人员和调查人员审查内容并确定您的视频是否有助于他们。简而言之，您越是有意为审核人员制作，他们就越有可能观看您的视频。

[image]

第二部分

如果您的视频没有得到适当的保护，您的视频的可信度就会受到质疑。以下基本步骤将帮助您保护原始文件的完整性，防止其被编辑或进行数字操作，用于避免设备故障、丢失或被丢弃、或可能落入坏人手中。

第一步

为了在现场的保护想出一个计划，以保护您的存储卡免受物理损坏，

防止坏人可能抢走您的镜头。在现场时，请考虑以下做法：

- 使用空白卡换掉旧卡并藏好使用过的卡;
- 即时创建备份;
- 立即将镜头上传到安全服务器;
- 不使用时，将存储卡存放在坚固、无尘的卡片盒中。

第二步

在您从现场返回后想出一个保护您的镜头安全的计划。请考虑以下做法：

- 在传输视频之前，在存储卡上设置写保护锁;
- 将原始文件从卡传输到硬盘驱动器而不以任何方式处理视频，以保存原始文件。不要通过特殊软件运行它或更改文件格式、文件名或文件结构;
- 如果可能，至少备份原始文件一次和两次。复制后，请勿以任何方式更改原始文件;
- 将备份副本保存在单独的设备上，并保持主副本位于不同的物理位置;
- 限定只有必须的人才能以物理和数字形式访问您的视频，以保持存储安全。

第三步：整理您的视频

如果您想整理从相机中导出的视频，请按日期和创建者格式将它们整理到文件夹中。

同样，请勿更改原始视频的格式、文件名或目录结构。以标准化方式命名您的文件夹，以便您可以轻松对其进行排序和识别，例如，yyyy-mm-dd_Creatorname_IncidentDescription。

第四步：跟踪视频

使用电子表格或数据库来跟踪存储素材的位置以及与之共享的人员。为了将您的视频用作调查的一部分，您需要将其提供给值得信赖的人权研究人员或调查人员。

当您将镜头提供给其他人或组织时，他们可能会要求您签署一份表格，记录手中的镜头。在法律方面，表格记录了“监管链”。请求的信息会有所不同，但您很可能需要验证您是否是视频录制者，并且未更改过视频文件。

目标

如果您认为在线分享视频片段是安全的 — 并且具有战略意义 — 请遵循以下基本实践，以便：

- 记者、研究人员或调查员能够搜索、查找、理解和验证您的视频;
- 让您使用的在线平台知晓该视频包含信息丰富的人权内容，这样它们就不太可能删除视频（YouTube 有所谓“暴力”内容审查）。

[image]

标题

将视频上传到在线平台时，请添加一个简短标题，其中包括日期、具体位置、城市、国家/地区，以及一些关于视频内容的关键描述性文字，要简明扼要。

说明

重复添加时间、日期、具体位置、城市和国家/地区的事实描述，并包含视频中显示内容的事实摘要。添加文字有助于观众了解视频的上下文，例如录制之前或之后发生的事。避免个人意见、错误信息和夸大描绘。如果确认安全，请包括摄像师或摄像师组织的名称和安全的联系信息。

关键说明

上传时请标注图像视频属于＜人权内容＞。这将：

- 提醒观众视频可能存在暴力或令人不安的画面;
- 在线平台发布时，提醒视频片段可能包含有价值的人权镜头，非常重要。如果没有此警告，YouTube 和其他平台可能会删除“违反其社区准则”的视频，该准则禁止用户发布没有公共价值的令人震惊、耸人听闻或不尊重的内容。

再次标签、日期、时间、具体位置、城市和国家/地区，然后添加描述性内容的关键字。例如：“人权”，“驱逐”，“逮捕”，“过度武力”，“炮击”，“抗议”，“儿童兵”，“检查站”，“制服”，“石油泄漏“，”折磨“或”难民“等，标签必须是公正的和描述事实的。

第四步：保存

文件视频网站（如 YouTube 等）非常适合分享视频，但不应将其用作保存视频原始副本的地方，因为：

- 上传到 YouTube 等平台的视频针对网络流式传输进行了优化，这意味着原始视频被压缩并可能剥离有价值的信息 — 文件中嵌入的元数据;
- 上传后您无法从 YouTube 等网站检索原始文件，因为只有针对网络流媒体优化的副本才可用;
- YouTube 和类似网站可以在未经您许可的情况下移除您的镜头，如今的审查已经越来越严重。

第三部分：与可信赖的个人和组织共享

第一步

与人权组织、调查员、执法人员和法院分享录像和信息会触发权利和责任。具体的权利和责任取决于您与谁共享信息。在将镜头提供给中间人进行保管之前，请务必选择以下中间人：

- 你确保能信任的人;
- 拥有技能、资源和基础设施，可以确保您的视频安全、完整和可靠的人;
- 尊重（甚至以书面形式保证）对镜头的具体使用的人，特别是不会给您拍摄到的人或社区组织带来安全风险的人。

第二步：决定如何提供原始文件给您信任的盟友以确保不会被更改

如果您与之分享视频的人或组织距离较近并且可以走访，则分享视频的最安全方式是亲自将视频从您的计算机或硬盘上传输给他们。但通常情况并非如此，将镜头传递给你的盟友的最常用实用方法是将通过网络。

如果您处于高风险状态，上传文件可能会很危险，于是需要选择相当安全的传输视频渠道（请参阅下面的技术推荐）。最好在选择通讯服务之前与您的盟友讨论安全风险。

第三步；提供补充信息

在可能的情况下，还需提供以下内容的印刷版或电子摘要：

- 视频捕获的时间、日期和具体位置;
- 视频中显示内容的简明事实摘要;
- 摄像师的姓名和联系信息、拍摄人员、以及可能掌握有关事件的宝贵信息并愿意与NGO或调查员交谈的其他人;
- 任何安全信息，确保您的盟友知道哪些信息是保密的，哪些信息可以与他人共享。

最后

考虑使用技术来保护您的视频。

虽然使用技术工具来增强视频的证据价值并不是强制性的，但是有用的新工具一直在开发中。这些工具与您的实践技能相结合，可以增强视频的可信度。以下是一些可供选择的选项。

捕捉：在现场拍摄、并可以为您的视频添加上下文

- Storymaker: 一款带有使用培训和模板的 Android 应用程序，可帮助您安全有效地随时随地捕获视频 — storymaker.cc

- InformaCam: Android 应用程序，用于通过嵌入式元数据创建安全且经过验证的视频，以确保捕获的镜头具有增强的证据价值 — guardianproject.info/informa

- eyeWitness: Android 相机应用程序，可记录和嵌入元数据，以方便法院对镜头进行身份验证及使用其作为证据 — eyewitnessproject.org

- Taggly: 同时适用于 Apple 和 Android 设备的应用程序，将使用元数据水印为您的媒体标记 — tagg.ly

保存: 保持媒体的安全和有序

- Seagate Wireless Plus: 便携式硬盘驱动器，电池供电，支持 Wifi，随时随地为您提供额外的存储空间。

- Syncme: 自动同步文件的 Android 应用。与 Seagate 配合使用，可以在现场不断备份您的资料

- Adobe Bridge: 媒体浏览工具，可帮助您整理视频，添加标签以及查看和编辑元数据。

- Activists’ Guide to Archiving Video: WITnESS 指南概述了存储

和编录视频的工具和最佳实践 — https://archiving.witness.org/archive-guide/

Share: 与他人分享时，请确保您的资料安全且私密

- Bittorrent Sync: 从一个设备直接传输到另一个设备，是在低带宽环境中进行安全共享的一个很好的选择 — getsync.com

- SpiderOak: 易于使用的“云端”存储，具有端到端加密功能，有助于提高文件共享的安全性 — spideroak.com

- BoxCryptor: 免费服务，在您将文件上传到 Dropbox 或其他“云”服务站点之前对其进行加密 — boxcryptor.com

好啦，以上是最为基础的技术技巧介绍。如果您拥有相关实战经验、遇到过本文中没有提及的难题或挫折、或者还知道其他更好的并方便可用的技术，欢迎在评论栏中与大家分享。

[image]

随时可在本站 工具-Tools 专题中搜索您需要的开源自由软件解决方案。

[image]
[image]

当你手握真相：最基本的防护知识

[image] 关键词	传输安全 元数据 加密 反审查 反追踪 存储安全 独立调查
[image] 关联	[image]如何安全地留住证据：给真相的记录者一些技术技巧建议；[image]给公民记录者的技巧指南；[image]公民取证技巧：如何留住真相？；[image]数字技术限制和最佳实践
[image] 创建时间	2025年3月4日
[image] **Description**	行动安全性

真相是危险的东西，这在任何国家都一样，撒谎是每一种权力稳固自身的通用方式。正因为如此，真相是捍卫民主的最有力武器。当您手握真相时，安全保护是非常关键的基础部分。

- Table of Contents

基本规则
在计算机上
1、Tor browser
2、Bitlocker (Windows) FileVault (MacOSX)
在脑子里
私下共享文件
1. 设置匿名电子邮件帐户：
2. 使用临时文件共享服务
3. 元数据
在您的设备上保持材料安全
a）永久删除文件：
b）远程擦除：
如何仅擦除 Intune 托管应用中的数据？
创建擦除请求

监视擦除请求
删除擦除请求 — — 非常重要
对于手机的远程擦除
在社交媒体
1、在攻击发生前：
2、在攻击期间
Doxxing
在攻击之前
在攻击期间
在社会上

[image]

本文不仅提供给在职记者，也包括公民记者，所有手握真相的人。真相是危险的东西，它会激怒作恶的人，尤其是不择手段作恶的人，他们会不惜一切地阻止真相的曝光。

但是很多人依然不重视这个问题，当我们谈论安全防护时总会听到一些记者这样回复：“我没有什么可隐瞒的”；或者：“反正我也不写任何敏感的东西“……但本文面向的就是普通记者和任何公民记者，如果是参与透明度革命的深度调查记者，则需要在保护层面做得更多。

作为普通人，请考虑一下：你会写一些可能让某人感到不安的东西吗？因为更常见的状况是，对手会试图通过散播你的个人、家人、财务等隐秘信息来恐吓你或羞辱你。这种事可能很难彻底避免它，但你完全可以通过自我保护让攻击变得足够难。

一直以来，我们大多数人都没有足够的知识、经验或时间来真正了解对我们的隐私至关重要的技术细节。本指南介绍一些更容易获得的措施和解决方案，至少可以减少您的脆弱性。因为隐私保护通常与锁自行车的工作方式相同：你只需确保自己的锁比您旁边的自行车更坚固。

[image]

激进社区用户请从这里进入：[image]数字技术限制和最佳实践

组办入门级培训请从S01开始：[image]S01整体安全 - 总章节：前线安防入门课

基本规则

请注意，这些解决方案的使用仅在技术上有所帮助 — — 它不能减轻我们对良好实践的需求（例如，确保不打开可疑的附件和可疑链接，尤其是来自未知发件人的链接；不要安装来自未知生产商的应用程序等等）。最后但同样重要的是：计算机和手机都应该配备最新的防病毒软件。

还必须记住，不要对不同的服务使用相同的密码，以及选择一个安全的密码，它不能是单词组成的，而是一个由大小写字母、数字和特殊字符的组合。

另一个相当不错的解决方案就是在您的计算机和手机上使用密码管理器（如 LastPass.com或 1Password）在所有设备上都适用。不幸的是，这也是存在风险的，尤其是对敏感人士来说，因为最终，如果有人抢走了您的计算机或管理员密码，那么就能立即获取您的所有密码。

我们现在专注于监控的主要威胁，但不关注公司的广告或跟踪 — 因此不会讨论像 Adblock，Adblock Plus 这样的应用程序（虽然更好的似乎是 uBlock Origin），还有 Privacy Badger，uMatrix 或 Ghostery，但绝对鼓励您比较它们并选择合适您的方案使用它。

还有一件事。在您能够使用 Wifi 之前许多公司需要自定义安装证书（弹出窗口说：'点击此处接受'）。您必须记住，即使站点使用了安全的 https 连接，它也可能使我们暴露在监控中（有时因为提供 WiFi 的公司要求监控所有流量）— 简而言之，如果您使用带有自定义证书的 Wifi，那么就关闭 wifi 进行机密传输，一般情况下，当你真正想要确定连接时，总是使用VPN。

[image]

基本规则汇总：[image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

以及：[image]一句话安全须知：记住这些句子，以简单地优化您的安全性

在计算机上

1、Tor browser

适用于 Windows，Mac，Linux 的免费浏览器，可防止第三方（例如您的 ISP）跟踪您的浏览历史记录。它对阅读特别有用，而不是积极参与，因为那时你仍然会提供信息。

它还避免了各方确定您的位置。

值得记住的是，不要用它登录 **Google** 帐户，否则您的搜索信息仍将被谷歌记录（所以您应该使用的是 **DuckDuckGo** 或 **StartPage** 这样的搜索引擎）。

我们推荐过挂 Tor 登陆 Twitter、Facebook 等老大哥平台，但是要知道，由于 Tor 的三级跳隐藏性，您的账户很有可能因此被这些老大哥公司视为可疑。您大概会经常遭遇要求验证手机的状况。

[image]

返回：[image]使用Tor保护自己时千万不要做这9件事

返回：[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09

2、Bitlocker (Windows) FileVault (MacOSX)

从政府的大规模监控、到普遍的在线跟踪、再到网络犯罪分子，危险无处不在。但有一种明显的方法可以缓解各种隐私威胁：那就是加密。

请记住奥巴马三年前所说的话："在任何情况下，我们都不希望真正强大的加密"。他非常诚实，因为好的加密能够给他们这些老大哥制造足够的麻烦。并记住斯诺登说过的话："加密会有效。正确实施强大的加密是您可以信赖的少数抵抗方法之一。"

当您试图保护自己的隐私时，可能完全不清楚该如何开始使用加密。但一个显而易见的起点是，隐私优势很高、技术学习曲线很低的方法，即所谓的全盘加密。只需要很少的工作量就可以开始使用。

如果你想加密硬盘并让它真正有助于保护你的数据，就不应该只是打开加密功能; 而是应该了解磁盘加密保护的基础知识，不保护的内容以及如何避免可能让攻击者轻易绕过加密的常见错误。

- 那么什么时候磁盘加密无效？

有一种常见的误解，即加密硬盘会使您的计算机安全，但这并非完全正确。事实上，磁盘加密仅对有物理访问您计算机的攻击者有用。它并不会使您的计算机更难以受到通过网络进行的攻击。

攻击者仍然可以利用社交工程学欺骗您安装恶意软件，您仍然有可能访问了恶意网站，等等无数被入侵的形式。当然，磁盘加密对阻止互联网监控也没有任何作用。像 NSA 这样的间谍机构，可以利用构成互联网骨干的光纤电缆，几乎可以监视你在网上做的所有事。需要完全不同的加密类别来解决该系统性问题。

但是现在重要的是要知道磁盘加密可以防止单一攻击：物理访问。磁盘加密的目标是，如果不是您本人的某个人访问您的计算机，比如抢走设备的警察，他们将无法访问您的任何文件，只会看到乱码，无用

的密文。

BitLocker 和 FileVault 只是最懒的解决方案。更好的选择是免费开源程序 VeraCrypt（适用于 Windows，MacOSX，Linux）。它绝对是无价的，特别是如果你使用几个不同的系统并有特定的愿望的话。

在脑子里

作为记者，您将记录、存储和传输大量的材料。这些材料中的一些可能是很敏感的。如果不希望曝光它们的人知道你持有这些材料，您和您的信息源都会陷入危险。

您应该采取措施确保敏感材料的安全存放，并且不会使自己或自己的来源处于危险之中。

最佳实践：保护您的材料：

- 查看材料的内容并评估是否可能使您或您的资源受到威胁；
- 评估您与之联系的人的身份是否会使您或他们面临风险；
- 考虑一下您的存储选项。您应该权衡将材料保持在线（在云端）或硬件（如硬盘驱动器或 USB）上是否更安全；
- 考虑传输或发送材料的最佳选择。请勿通过社交媒体网站发送您不希望公开的敏感材料或线索；
- 加密您的设备和文件；
- 了解元数据，及其如何使您面临风险。元数据的示例可以包括在线消息的发送者和接收者的时间、位置和联系细节。

对于元数据的具体方案，接下来我们会有一个系列文章详细讲述，关于如何利用，以及如何防止被他人利用。

私下共享文件

您可能需要通过网络与他人共享敏感文件，但这可能会使您和其他人面临风险。以下是有关如何更安全地共享文件的一些提示。

1. 设置匿名电子邮件帐户：

您可能想要设置一个与您的身份完全无关的电子邮件地址。如果您这样做，您写信的人也应该设置一个与其身份完全无关的帐户。

研究您的电子邮件服务商，使用不在您或您的联系人管辖范围内的电子邮件服务提供商。

确保电子邮件服务提供商的所在国家/地区拥有强大的隐私权法律，并检查公司记录的信息。元数据可以包含诸如 IP 地址之类的信息，您应该希望公司尽可能少地保留元数据。

检查公司是否使用 SSL 连接，如果不是那就不安全。在此处输入您要查看的网站的网址，检查站点的 **SSL** 详细信息。需要 **A** 或 **B** 等级才行。

连接到匿名电子邮件服务器时使用虚拟专用网络（VPN），而且不要在能识别您身份的地点使用 VPN（比如办公室或家）；检查电子邮件服务提供的邮件存储量，并评估它是否足以满足您的需求。

加密文档和文件。

切勿将帐户链接到您的任何其他帐户或将其用于任何其他目的。使用完毕后始终删除帐户。

2. 使用临时文件共享服务

如果您不想设置匿名加密电子邮件帐户并且无法亲自与某人见面，则可能需要使用临时文件共享服务。这些服务允许您发送文件而不将其链接到您的身份。

常用的临时文件共享服务包括： **Firefox Send** 、 **Onion Share**

3. 元数据

您的文件可以存储诸如姓名或姓名缩写、公司或组织名称、和/或计算机个性化信息之类的数据。还可以保存有关从中复制文件的网络或其他计算机的详细信息，任何文件编辑者或贡献者的姓名以及编辑历史记录等。

图像和视频则包含大量有关所用摄像机类型的数据，以及创建图像或视频的时间、日期和位置，您的设备信息等，大量与您的身份相关的信息。

注意： 如果处理敏感报道，请使用与您完全无关的设备。

通过将文档和照片上传到 **Exifdata** 来测试哪些元数据存储在文档和照片中。不要将任何敏感材料上传到网站; 而是使用不包含重要内容的文件。

您可以使用适用于 iOS 的应用程序，检查使用 iPhone 拍摄的照片的元数据，这里：iPhone。

您可以通过 Chrome 和 Firefox 浏览器上的附加功能检查 Internet 上找到的图像文件的 exif 元数据：Exif add for Firefox 、 Metadata on add for Chrome

您还可以采取措施从材料中删除元数据。以下内容可用于执行此操作：

- 对于Microsoft Office，请使用 Document Inspector。
- 对于 Android 照片和视频，请使用 ObscuraCam。

[image]

可在本站 工具-Tools 专题中搜索“元数据”，查找可能更适合您的开源自由软件。

在您的设备上保持材料安全

a）永久删除文件：

从垃圾箱中删除的材料会保留在硬盘驱动器上，并可以被恢复。要确保永久删除材料，您需要重新擦除文件。您可以使用许多工具来执行此操作。

永久删除文件的工具 — 橡皮擦：适用于 Windows 的；适用于 Mac 的永久橡皮擦。

[image]

返回：[image]定期清理硬盘

返回：[image]这些使用暗网的人是如何被抓到的？: 总结教训

返回：[image]来自人身的威胁：如何在敌对环境中保护自己 S02E01

b）远程擦除：

有时可能会丢失设备或者设备被抢走。为了保护您的材料和数据并将风险降至最低，您应远程擦除计算机上的内容。

[image]

返回：[image]如果您的手机被盗或被警察抢走...

返回：[image]如果您的手机被盗了或被警察抢走了，怎么办

返回：[image]在坏人强行访问您的设备的情况下抹除数据

返回：[image]取证和反取证工具及资源

如何仅擦除 Intune 托管应用中的数据？

这里可以删除从应用直接同步到本机通讯簿的联系人。 无法擦除从本机通讯簿同步到另一个外部源中的任何联系人。目前仅适用于 Microsoft Outlook 应用。

创建擦除请求

- 登录到 Azure 门户。
- 选择“所有服务”，在筛选器文本框中键入“Intune”，然后选择“Intune”。 Intune 窗格随即打开，选择“客户端应用”窗格。
- 在“客户端应用”窗格中，选择“应用选择性擦除”。
- 选择“新建擦除请求”。 “新建擦除请求”窗格打开。

- 选择用户，然后点“选择”，以选择你要擦除其应用数据的用户。

- 然后，从“新建擦除请求”窗格中选择“设备”。 此操作会打开“选择设备”窗格，其中列出了与所选用户关联的所有设备，还提供了两个列：“设备名称”（用户定义的友好名称）和“设备类型”（其设备平台）。 选择要擦除的设备。

- 现在已返回“新建擦除请求”窗格。 选择“确定”以提出擦除请求。

- 服务会为设备上的每个受保护应用以及与擦除请求相关联的用户创建并跟踪单独的擦除请求。

监视擦除请求

您将获得一个汇总报表，其中介绍了擦除请求的总体状态，并包括挂起请求数和失败次数。 若要获取更多详细信息，请按以下步骤操作：

- 在“客户端应用 — 应用选择性擦除”窗格中，可以查看按用户分组的请求列表。 由于系统会为设备上运行的每个受保护应用都创建一个擦除请求，因此对于某个用户，你可能会看到多个请求。 状态指示擦除请求是“挂起”、“失败”还是“成功”。

- 此外，还可以查看设备名称及其设备类型。

- 用户必须打开应用才能进行擦除，进行请求后可能需要最多 30 分钟才能完成擦除。

删除擦除请求 — — 非常重要

手动删除擦除请求：

- 在“客户端应用 — 应用选择性擦除”窗格上。
- 从列表中，右键单击要删除的擦除请求，然后选择“删除擦除请求”。
- 系统将提示你确认删除，请选择“是”或“否”，然后单击“确定”。

远程擦除 iCloud 就非常简单了，见苹果的帮助页面。

对于手机的远程擦除

从 Android 2.2 开始，远程擦除已经成为操作系统的一项功能。必须通过 Exchange 服务器或中央 Google Apps 帐户启动远程擦除。如果您是独立或小型公司从业者，或者您只是独立于办公室使用该设备，您可能需要安装第三方应用程序才能启用远程擦除。

这个功能的两个流行的应用程序是：

Android Lost （免费）

允许用户通过互联网或短信远程控制 Android 手机。可以用它来阅读短信收件箱/发送短信，擦除手机，锁定手机，找到设备等等。

Where’s My Droid Pro （3.99美元）

就是类似「Find My iPhone」的程式。

如果是黑莓可以安装 RIM 提供的应用程序：BlackBerry Protect。该应用程序通过 BlackBerry AppWorld 下载，安装后您将能够无线备份设备，锁定或擦除其内容，通过 GPS 定位设备，并快速将设置和数

据恢复到新设备。

但是要知道，无论是 Apple 或是 google Android 的寻找手机程式，都是防君子不防小人的，如果有目的的人拿到您的手机，只要立即移除该 Wheres My Droid 程式，或是关闭 Wi-Fi 或 3G 行动上网的话，这些都会不起作用。所以还要看运气，并且您的动作要尽可能快速。

在社交媒体

TROLLING 和 DOXXING 是最常见的。社交媒体对于记者来说已经变得越来越重要，作为促进他们的工作和发表意见的工具。这便也导致了 trolling 形式的在线滥用程度增加。

Trolls 可以是真人或机器人运行的虚假账户。他们有几个目标。一是通过留下非常多的评论以淹没正常的讨论，使记者无法参与对话。另一种是恐吓或威胁记者。并且在某些情况下，trolls 可能会试图入侵记者的账户。一旦记者被确定为 trolling 的目标，上述状况随时可能会发生。

[image]

返回：[image]给活动家的反人肉指南

返回：[image]如何知道有人正在线人肉你？6个简单的方法

当记者涉及某些政治问题，或政治、人权、种族、女权主义和妇女权利等问题时，非常可能成为 trolls 的目标。重要的是要确定 **trolling** 的原因和 **trolling** 的目的，以保护自己。

分为两部分。

1、在攻击发生前：

- 通过创建安全的加长密码和/或考虑使用密码管理器来保护您的帐户免遭黑客入侵；

- 为您的帐户启用双因素验证。如果有人试图破坏您的帐户，系统会提醒您；

- 查看社交媒体帐户的隐私设置，并锁定您不希望公开的任何信息；

- 在线筛查您的照片，并评估使用这些照片是否会被用来诋毁您。Trolls 经常盗用在公共领域中发现的图像，并将其用作玷污记者形象的一种方式。这些图像通常是完全正常的日常照片，但是您应该用攻击者的视角来判断它们，一旦有可能，请立即删除；

- 定期查看您的社交媒体网站，以及时掌握可能表明 trolling 情况开始的评论。在报道发表之后要特别警惕，特别是如果它是一个吸引 trolls 兴趣的话题的话。

2、在攻击期间

- 当发生 trolling 时尽量不要与攻击者交战，因为这会使情况变得更糟；

- 看看 trolling 的类型（真人还是机器人），并试图确定谁是背后的人；

- 您可能想要阻止或静音 trolls。您应该向社交媒体公司报告任何辱骂或威胁的 trolls。更改Twitter上的设置以控制您在Feed上看到的内容；

- 如果 trolling 涉及诽谤您的角色和/或您的工作，请考虑动员一组支持者在社交媒体上联合抵制；

- 如果攻击特别糟糕，您可能需要考虑下线；

- 考虑让您的编辑和主要工作联系人了解情况；

- 记录攻击。有关如何执行此操作，请参阅 TrollBusters 在线骚扰指南（下图）。

[image]

延伸：https://iyouport.substack.com/p/as29-trolling-doxing-2?utm_source=publication-search

[image]

Doxxing

Trolling 攻击也可能涉及 doxxing，发生在个人信息（例如地址或电话号码）在线公开的时候。此信息通常来自公共数据库或记者的在线资料。攻击者还可以破解您的帐户以获取个人数据。然后，该信息被用作骚扰和/或恐吓记者的方式。这可能会有不同的威胁程度，从电话骚扰到拦路威胁等等。

在攻击之前

- 查看您的在线个人资料，最好使用 OSINT 的方法筛查包含有关您和您家人的个人信息的网站，例如搜索目录和名册等。您可以删除这些信息，这取决于不同国家的网站和法律，比如在美国就可能需要花钱，在欧洲不需要；

- 删除社交媒体网站和网站上公开的联系方式和个人数据，例如您的出生日期等。为与您联系的一切人创建仅限工作使用的电子邮件地址；

- 锁定社交媒体帐户上的隐私设置。记住对手有可以通过您的家

人和朋友的账户获取大量信息；

- 为您的帐户创建强密码；
- 查看您帐户中的内容，包括社交媒体上的电子邮件和私信，以获取可能会使您面临风险的任何信息。如果可能的话，删除任何可能会对您造成伤害的内容。

在攻击期间

- 如果您认为您或您家人的生命可能处于危险之中，请考虑重新安置。在这种情况下，Rory Peck Trust 等组织可能会提供建议和支持；
- 记录攻击并创建事件日志；
- 查看您的在线个人资料并删除所有个人信息；
- 更改常用帐户的密码。攻击者有可能尝试访问这些帐户；
- 让您的银行、公用事业公司和移动电话公司知道您需要防止欺诈性地使用这些服务；
- 让人们知道你已经被攻击，包括家人、雇主和您的朋友，告知他们小心。

在社会上

正如有许多不同类型的记者一样，也有不同类型的计算机程序员。

其中一些人致力于保护互联网言论自由，其中包括从事数字安全问题的技术人员。他们设计、构建和测试工具，以帮助人们在线保护自己。

这些计算机程序员通常喜欢透明度，是开源的支持者，以便其他人可以查看代码并查找错误。开源是一个绝好的标志，表明您使用的工具得到了技术社区成员的认可。

数字安全建议会定期更改，这对记者来说既困惑又麻烦。作为记者，重要的是要了解为什么会发生这些变化，并随时了解数字安全领域正在发生的事。

于是我们强烈建议您与当地的技术社区合作。计算机程序员、设计人员和数据专家经常会创建新工具，他们当然希望记者与他们合作并提供有关软件设计、可用性或其他方面的反馈。

就像自由撰稿人一样，一些计算机程序员经常很难通过工作获得足够报酬。许多项目通过赠款和捐赠来资助，或者在空闲时间无偿的服务。

社区间的联合能保证□家不会重复劳动、互相助益，并能有效的分□和协助，还能促进凝聚□和提升解决问题的效率。

[image]
[image]

如何识别抗议活动中可见的和不可见的监视

[image] 关键词	反监视 威胁响应 威胁识别
[image] 关联	自卫措施
[image] 创建时间	2025年10月1日
[image] **Description**	行动安全性

监视的目的是最有效地镇压、包括扼杀任何反抗动员，如果您希望自己参与的抗议活动能获得成功，至少没那么容易被消灭，您就需要警惕所有这些警察间谍手段……

- Table of Contents

可能可见的监控技术
1、身体相机
2、无人机
3、自动车牌读取器
4、移动监控拖车
5、**FLIR**监视相机
也许不可见的监控技术
1、人脸识别（或其他视频分析）
2、社交媒体监视
3、黄貂鱼
4、实时**(**打击**)**犯罪中心
最后

[image]

在反抗运动中，不仅有传统的防暴盾牌、催泪瓦斯和维稳战术的展示，而且，现代警务的数字化武器也出现了：丰富的监视技术不论是街头还是在线。

[image]

延伸：https://iyouport.substack.com/p/9b3?utm_source=publication-search

如果您准备参加抗议活动，请使用S05系列 [image] S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训。

本集内容是对监视技术的回顾，关于警察将会如何部署以镇压反抗运动。

可能可见的监控技术

1、身体相机

[image] 佩戴着身体相机的警察，资料来源：休斯敦警察局

关于身体相机的问题 https://iyouport.substack.com/p/a3b

与许多其他形式的警用技术不同，随身佩戴的身体相机既可作为执法功能，也可作为问责功能。警察佩戴的身体摄像机可以记录警察的不当行为和使用武力的情况，但是，录像也可用于监视警察与之互动的任何人和可能根本没有意识到自己被拍摄的第三方。

如果与人脸识别或其他技术相结合，数以千计的警察佩戴的随身摄像机可以在特定时间内记录大部分抗议者的言行和位置，这引起了第一和第四修正案的严重关注。因此，加州目前已经暂停在移动警务设备上使用人脸识别技术，包括身体相机。

[image] Axon Flex摄像头系统 来源：TASER Training Academy presentation for Tucson Police Department

身体相机有不同的款式，有些戴在胸前，有些是在警察的肩膀上，而在某些情况下，摄像机可能部分隐藏在背心下面，只有镜头露出来。

并且，还有一些公司在销售包含监视摄像头和人脸识别功能的战术眼镜，就像中国使用的那种。

[image] 警察背心上的扣子之间可以看到戴在身上的监视摄像机镜头。来源：Laredo Police Department Facebook

- 中国有这个东西吗？是的，有。

2、无人机

[image] Sahuarita 警察局在桌上摆放的无人机。Source: Town of Sahuarita YouTube

无人机不仅可以用来监视，还可以而且已经被用来镇压了。

[image]

返回： https://iyouport.substack.com/p/0c8?utm_source=publication-search

返回： [image]5种常用的“击落”无人机的方法

无人机可以配备高清晰度的实时视频摄像机、热红外摄像机、热传感器、自动车牌读取器和雷达，所有这些设备都可以进行复杂和持久的监视。

无人机可以在白天录制视频或拍摄静止图像，也可以使用红外技术在夜间拍摄此类视频和图像。它们还可以配备其他功能，如手机拦截技术，及其他软件工具，如车牌阅读器、人脸识别和GPS跟踪器。

[image]

返回：🚁空中监视

在美国，已经有人建议执法部门在无人机上安装致命性和非致命性武器。

无人机的大小不一，从小型四旋翼飞机 (又称sUAVs) 到大型固定翼飞机，如捕食者无人机。它们比普通飞机或直升机监视更难以被发现，因为它们更小、更安静，有时可以在天空中停留更长时间。

活动人士和记者也可以在抗议现场部署无人机，行使第一修正案的权利，收集警方对抗议者的反应信息。因此很难判断抗议现场出现的无人机究竟属于谁，所以也更危险。

- 中国有这个东西吗？是的，有。

3、自动车牌读取器

[image] Photo by Mike Katz-Lacabe (CC BY)

自动车牌阅读器 (ALPRs) 是一种高速的、计算机控制的摄像系统，可以安装在电线杆、路灯、公路立交桥、移动拖车或警车上。

ALPRs 自动捕捉所有进入视野的车牌号码，以及地点、日期和时间。这些数据包括车辆的照片，有时还包括司机和乘客的照片，然后上传到一个中央服务器。

[image] Photo by Mike Katz-Lacabe (CC BY)

在抗议活动中，警方可以部署ALPRs，以识别驶向、驶离或停在游行示威或其他公众集会现场附近的任何人。例如，CBP在一个由第二修正案支持者参加的枪支展上部署了一个ALPR拖车。

与城市周围的其他 ALPR 一起使用，警方可以跟踪抗议者从示威现场

到家的每一步行程。

■ 中国有这个东西吗？是的，有。

4、移动监控拖车

[image] A ‘Mobile Utility Surveillance Tower’ at San Diego Comic-Con and a mobile surveillance pole in New Orlean’s French Quarter

美国有数百个警察部门都有这种移动监控车，可以停放在抗议活动现场上方数层楼高的地方。

这些拖车通常配备有摄像头、聚光灯、扬声器，有时还有供警察使用的小型封闭空间。它们往往还具有自动报警功能。

常见的监控塔楼包括 Terrahawk M.U.S.T.，它看起来像安装在面包车上的警卫塔，以及 Wanco 监控塔，它是一个带有大型可延伸杆的卡车拖车。

■ 中国有这个东西吗？不知道，只因为没有在抗议活动现场看到过这个东西出现。但理论上中国应该有，因为这个东西很容易买到。

5、FLIR监视相机

前视红外（FLIR）摄像机是一种热像仪，可以读取人的体温，并可在夜间进行勘察。这些监视相机可以是手持式的，也可以安装在汽车上、步枪上或头盔上，并经常与飞机、直升机或无人机等空中监视结合使用。

■ 中国有这个东西吗？是的，有。

也许不可见的监控技术

1、人脸识别（或其他视频分析）

[image]

人脸识别系统可用于识别照片、视频或实时地识别个人。警察也可以在街上随机拦截过程中使用移动设备来识别个人的身份。

在抗议活动中，你遇到的任何监视摄像头都可能启用了人脸识别或其他视频分析功能。这包括警方的身体摄像机、安装在建筑物上的监视摄像机、路灯上的监视器、或拖车上的监控塔。

此外，一些警察部门有生物识别设备，如专门的智能手机和平板电脑，可显示被拘留者的身份。同样，在监狱和拘留设施的登记过程中，也可以进行人脸识别。

[image]

返回：🎭面部识别

- 中国有这个东西吗？是的，有。

2、社交媒体监视

社会媒体监视很普遍，特别是围绕抗议活动的监视，即 社交媒体情报。

[image]

返回：🔍开源情报

警方经常搜索社交媒体标签、热点事件、数字互动和联系、以及在线

组织团体。这可以由实际的人进行，也可以由经过训练的算法来收集含有某些标签、单词、短语或地理位置标记的社交媒体帖子。

警察会使用袜子木偶账户渗透到在线私密群组中进行监视，比如最臭名昭著的 “Bob Smith”。

■ 中国有这个东西吗？是的，有，都已经近20年了。 BACK [image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式

3、黄貂鱼

黄貂鱼已经在全世界泛滥。

[image]

返回：[image]黄貂鱼

操纵黄貂鱼的警察一旦识别出手机的IMSI，便可以尝试识别拥有这些手机的抗议者身份。

在没有抗议活动的情况下，警察也使用黄貂鱼来识别特定电话（及其所有者）的位置，其准确性通常比电话公司蜂窝站点位置信息的准确性更高。

■ 中国有这个东西吗？是的，有。

4、实时(打击)犯罪中心

[image] 弗雷斯诺警察局的实时犯罪中心。资料来源：弗雷斯诺警察局2015年年度报告

实时打击犯罪中心(RTCCs)是由警官和分析人员组成的指挥中心，负

责监测各种监控技术和数据源，以监视整个社区。

实时打击犯罪中心往往提供一个中心位置，用于分析ALPR馈送、社交媒体情报和监视摄像头网络，并为分析人员提供使用预测性算法[少数派报告技术]的能力。

[image]

返回：https://web.archive.org/web/20200518222001/https://www.iyouport.org/%E6%9C%AA%E6%9D%A5%E6%98%AF%E4%B8%80%E9%A1%B9%E6%96%B9%E7%A8%8B%E5%BC%8F-%E5%B0%91%E6%95%B0%E6%B4%BE%E6%8A%A5%E5%91%8A%E7%9A%84%E5%A8%81%E8%83%81%E4%B8%8D%E6%98%AF%E8%BF%99%E4%B8%A4/

返回：https://iyouport.substack.com/p/e1c?utm_source=publication-search

返回：https://iyouport.substack.com/p/viedo-526?utm_source=publication-search

- 中国有这个东西吗？是的，有。

最后

EFF 这篇文章分析的是美国的抗议者将面对哪些监视技术，但是，如您所见，其中提及的所有技术中国基本都有。换句话说，准备组织或参加抗议活动的中国公民，需要首先了解自己将身处的环境，以便提前做好准备。

您也许很勇敢可以说自己“不担心被监视”，但是监视的目的是最有效地镇压、包括扼杀任何反抗动员，如果您希望自己参与的抗议活动能获得成功，至少没那么容易被消灭，您就需要警惕所有这些警察间谍

手段。

[image]
[image]

如何躲避无人机 - 监视时代须知

[image] 关键词	反监视 大规模监视
[image] 关联	☠️镇压手段 ；🚁空中监视 ；⛑️自卫措施
[image] 创建时间	2025年10月2日
[image] Description	行动安全性

监视时代的基本生存技能……

- Table of Contents

  拥挤的天空
  如何从无人机的视野中消失
  随身携带一把雨伞
  总结

[image]

无人机有非常多的用途。

各种规模的无人机正被环保活动家用来监测森林砍伐，被保护主义者用来追踪偷猎，被记者和活动家用来记录大型抗议活动 …… 研究社会运动和无人机的政治社会学家 Austin Choi-Fitzpatrick 在他的新书《The Good Drone》中记录了无人机广泛的非暴力和亲社会用途。他认为，这些努力有可能使监视民主化。

但是，当国土安全部将大型固定翼无人机从美墨边境调往抗议活动现场进行监视、当城镇尝试使用无人机对人们进行体温检测 …… 是时候思考天空中有多少双眼睛了，以及如何避免不必要的空中监控。

一个几乎每个人都唾手可得的方法就是学习如何简单地从无处不在的监视器视野中消失。

[image]

激进社区用户请从这里进入：🚁空中监视

拥挤的天空

在过去的十年里，公众对无人机的使用呈爆炸式增长 —— 人们用日常科技做着有趣的事。随着无人机进入已经拥挤的空域，航空管理部门正在努力应对。在不久的将来，天空中可能会出现更多的这些设备，由越来越多的社会、政治和经济目标参与者推动。

公众对无人机的使用和扩大化的看法仍然悬而未决，但无人机使用的迅猛发展已经引发了许多限制无人机的努力，包括制定公共政策，让社区对当地空域进行控制，以及开发先进的干扰设备和战术，将无人机从天空中击落。

从初创企业到主要的国防承包商，都在争相设立拒绝无人机的领空，用数字技术劫持无人机、控制无人机、击落无人机。反无人机措施从简单的钝器、到10口径猎枪，再到训练有素的鹰。

这些反无人机措施很多都是昂贵而复杂的。有些是非法的。避免无人机技术的最实惠、也是最合法的方法就是：躲起来。

如何从无人机的视野中消失

要想躲避无人机，首先要利用自然和建筑环境。可以等待恶劣天气，因为像当地警方使用的小型设备很难在大风、浓雾和大雨中飞行。

树木、墙壁、凹槽和隧道可以比天气更可靠，如果您遇到的是国安部使用的那种高空无人机的话，这些物体可以帮助您躲避。

[image]

您可以做的第二件事是尽量减少您自己的数字足迹。尽可能避免使用手机或GPS系统等无线设备，因为它们有数字签名，可以揭示您的位置。这对于躲避无人机来说是很有用的，并且对于抵制其他很多监视技术来说也非常重要。

第三件您可以做的事就是迷惑无人机。在地面上放置镜子、站在破碎的玻璃上、戴上精致的头盔、使用机器可读的图案印制的毯子、或可以干扰传感器的布料制作的夹克，以破坏和扭曲无人机看到的图像。

人体模型和其他形式的模仿也能迷惑机载传感器和负责监控无人机视频和传感器信号的分析人员。

请注意，装有红外传感器的无人机会看穿人体模型的把戏，但也会被掩盖体温的策略所迷惑。例如，太空毯会掩盖大量的人体热量，或者简单地躲在与人体温度相匹配的区域，如建筑物或人行道的排气口，也能做到隐藏。

第四种，也是最实用的，那就是伪装。大规模监控的发展导致了旨在隐藏身份的创造性实验的爆发。但一些最聪明的想法显然是老派的和低技术含量的。衣着是首选，帽子、眼镜、面具和围巾对扰乱基于无人机的面部识别软件来说就能有很大帮助。

[image]

请记得，您的步态就像您的指纹一样独一无二。随着步态识别软件的发展，还必须考虑如何掩盖用于识别步行者的关键支点。可能最好的反应是一瘸一拐，使用轻微的腿部支撑或穿着极度宽松的衣服。

[image]

返回：[image]特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06

返回：[image]匿名着装

返回：步态识别

艺术家和科学家们将这些方法又向前推进了一步，开发出了一种旨在屏蔽一个人的热标记和扰乱面部识别软件的帽衫，以及旨在挫败面部识别系统的眼镜。

随身携带一把雨伞

上述这些创新都是很诱人的，但雨伞可能被证明是这个列表中最普遍使用的和最强大的策略。它们价格便宜，易于携带，并且可以在短时间内发挥作用。另外，如果您愿意，还可以打造一个高科技的雨伞，比如这种。

如果您生活的地方没有警察使用小型四旋翼飞机监视人们的生活、也没有国土安全部部署大型 “捕食者” 无人机来监视抗议者，那当然是极好的事；对于世界上某些地方的人来说，要小心别把无人机的声音和即将发射的导弹联系起来。但是如今全世界的人都应该知道，有那双眼睛在天上的存在，每时每刻都应该有所意识，明白该如何躲避它。

总结

以下是美国军方介绍的几种躲避无人机的方法：

1. 白日伪装：躲在建筑物或者树木的阴影里。利用茂密的树林作为天然遮蔽或使用伪装网；

1. 夜晚伪装：躲在建筑物中或者茂密的树叶下。禁止使用手电筒或者车头灯，哪怕仅是对准远方。无人机可以在夜间任务中轻

而易举地识别出灯光；

1. 热伪装：聚酯薄膜（Mylar）制成的急救毯可以隔绝红外线。在夜间把急救毯作为披风穿在身上可从红外探测中隐藏您的热信号。在夏天，当气温在36至40摄氏度之间时，红外摄像头无法从周围环境中辨别人体；

1. 等候恶劣天气。无人机无法在大风，烟雾，暴雨，等恶劣天气条件下工作。

1. 禁止使用任何无线通信。使用移动电话或者全球定位系统（GPS）可能会暴露您的方位。

1. 迷惑。在车上或屋顶上散布反光玻璃碎片或者镜面反光材料可以搅乱无人机的摄像头。

1. 使用诱饵。使用人体模特或者真人大小的玩偶来误导无人机的侦察。

无人机是被遥控的。无人机操作员们可以坐在千里之外的地面控制站里，可以由驾驶员通过卫星传递数据来操控飞机。通过堵塞或者截取数据连接，就可以干扰无人机的操控。数据链可被加密但常常没有加密。

1. 截取信号。复杂技术是通过SkyGrabber软件、卫星天线和调频器来截取无人机的通信频率。

1. 干扰。通过广播不同的频率或者一组频率，无人机操作员和无人机之间的连接可以被切断。

1. **GPS**欺骗。小型便携式GPS发射器可以发出虚假的GPS信号来扰乱无人机的导航系统。这种方法可以被用来引导无人机进入自毁的飞行路径，或者劫持它们逼迫其降落。

[image]

警察如何利用抗议者的手机追踪每个人

[image] 关键词	免追踪 街头 追踪
[image] 关联	[image]匿名手机 ；[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03 ；[image]你的手机如何背叛了民主？
[image] 创建时间	2025年10月3日
[image] **Description**	行动安全性

完全不需要大规模的反抗运动，即便在日常状况下，您也很有可能被同样的大撒网监视方法所捕获。所以不论您是不是反抗者，都应该了解这些事。本文的 “谷歌”，在中国就等于百度和高德。

- Table of Contents

  1、什么是地理围栏监控
  2、警察多久使用一次这些数据？
  3、如何知道您自己是否已经被地理围栏搜查捕捞？
  4、警方有多容易获得这些搜查令？
  5、这些手令是否受到立法者的挑战？
  6、这些数据会被误读或具有误导性吗？
  7、如何防止我的数据被这样收集？

Edward Snowden: "Both Apple and Android devices unfortunately are not especially good in protecting your privacy."Every phone, even when the screen is off you think it's doing nothing, but it's screaming 'Here I am'.""They can see everything about you. They

can see everything about what your device is doing, and they can do whatever they want with your device.”
attachment:1e1f89d8-073a-43b7-8e2a-9860423e6935:cXRgqikhBzdSUR_F.r
[image]

如今的警察监控大多不再瞄准单一的目标人，而是设置地理围栏 —— 在地图上画一个圈，偶然出现在这个圈儿里面的任何人都会被纳入监控。

利用这些范围广泛的数据请求，警方经常从谷歌等寡头公司获得信息，收集当时在该地区（那个圈儿里面）的任何人的数据，而被牵连进去的几乎所有的人都是无辜的。甚至重大案件如凶杀案，警察也这么干。

与此同时，在明尼阿波利斯市 George Floyd 被警员杀害所引发的对警察暴行的抗议活动后，全国已有上万人被捕。BuzzFeed 新闻报道称，缉毒局已被授权对抗议者进行监视。

地理围栏监视，有时也被称为反向地理定位搜索，只是其中的一种工具。它们有效地允许警方通过一个单一的请求就能获得每个抗议者的信息。

谷歌因为其位置追溯功能而令警方可以获得这些请求中的大部分满足，谷歌称它只提供已经加入该功能的用户的数据，这需要选择加入。

“我们大力保护用户的隐私，同时支持执法部门的重要工作。我们专门为这些请求制定了一个流程，旨在履行我们的法律义务，同时缩小披露数据的范围”，谷歌的执法和信息安全总监理 Richard Salgado 在一份声明中说。

说的真好听。“隐私” 成为了羊头的狗肉，不要上当。

[image]

返回：https://web.archive.org/web/20191029121133/https://

www.iyouport.org/%E4%BB%A5%E9%9A%90%E7%A7%81%E4%B8%BA%E7%9B%AE%E7%9A%84%E7%9A%84%E6%96%97%E4%BA%89%E5%A6%82%E4%BD%95%E8%AE%A9%E4%BD%A0%E5%8F%98%E6%88%90%E4%BA%86%E7%9B%91%E8%A7%86%E7%9A%84%E7%9B%9F%E5%8F%8B/

返回：https://web.archive.org/web/20200809084114/https://www.iyouport.org/%E5%9C%A8ces%E4%B8%8A%EF%BC%8C%E6%8A%80%E6%9C%AF%E5%AF%A1%E5%A4%B4%E6%AD%A3%E5%8A%AA%E5%8A%9B%E5%AE%A3%E6%89%AC%E9%9A%90%E7%A7%81%EF%BC%8C%E4%B8%8D%E8%A6%81%E7%9B%B8%E4%BF%A1%E4%BB%96%E4%BB%AC/

请注意，谷歌没有就是否会遵守与追踪抗议者有关的地理围栏搜查令发表评论。

警察监视公众的工具数量空前，促使技术人士制定了多份关于在参加抗议活动时保护隐私的指南。

警方过去也曾使用过类似的手段来识别示威者的身份。EFF获得的记录发现，加州大学警方向电话供应商发出搜查令，以确定2017年加州大学伯克利分校抗议活动中的示威者的电话号码和姓名。

“想象一下，这种工具可以如此轻易地被用来识别抗议活动中的每一个人，无论他们是否违法或有任何不法行为的嫌疑，这会让人不寒而栗。” 监视技术监督项目执行主任 Albert Fox Cahn 说。

以下是对地理围栏监控的分析，它们被使用的频率，以及如何找出您本人是否已经成为这些扫荡式监控策略的一部分。

1、什么是地理围栏监控

地理围栏搜查令是警方向科技公司发出的关于特定区域内所有设备信息的搜查令。

通常情况下，搜查令本应该是在有正当理由的情况下进行的，并与特定的嫌疑人或地址挂钩。但是，地理围栏搜查令允许跨区域进行全面搜查，并且不需要正当理由，甚至不需要知道嫌疑人是谁。

如果一家公司遵守搜查令，它就必须提供特定区域内所有设备在特定时间的详细信息。这意味着警察不仅会获得他们认为是嫌疑人的人的数据，还能获得在同一时间碰巧出现在同一地点的所有人的信息。

其中很多请求都是发给谷歌的，因为安装在25亿台活跃设备上的安卓操作系统比苹果的iOS系统更加普及。谷歌也有一些应用，比如谷歌地图，普及率非常高，可以收集安装在任何设备上的数据 —— 包括苹果产品。

虽然警察可以向任何公司发出请求，但很多公司并不像谷歌那样拥有广泛的覆盖面和位置数据保留。

向谷歌发出的地理围栏搜查令请求，要求从其 Sensorvault 数据库中获取信息，该数据库拥有数亿人的位置记录。该数据库旨在用于谷歌的广告目的，但是，警方正越来越多地将其用于追踪任何人。

为了遵守这些要求，谷歌会针对数百万用户进行搜索，以确定他们是否在警方调查的时间段内出现在某个地点附近。

“殖民时代的一般手令授权执法部门可以挨家挨户寻找证据”，Rumold 说，“而现如今你要逐个搜查谷歌用户，搜索他们的位置记录。这是史无前例的。”

结果会返回一堆ID号。然后，警方会挑选某些他们认为可疑的设备，以获得更具体的信息。

在2019年12月的一份法庭文件中，谷歌表示，**Sensorvault** 数据库提

供的数据往往比电话塔的定位记录更准确。这是因为它的位置数据并不只来自一个来源，而是GPS信号、Wi-Fi网络、蓝牙信标和手机塔数据的组合。

2、警察多久使用一次这些数据？

地理围栏搜查在警察中越来越受欢迎。

从2017年到2018年，对谷歌的地理围栏搜查请求增加了15倍。该公司在法庭文件中表示，第二年，这个数字又增加了五倍。纽约时报2019年4月的一份报告发现，谷歌每周收到的请求多达180次。

据《福布斯》2019年12月的报道，在酒精烟草火器和爆炸物局（ATF）的调查中，谷歌提供了反向定位搜索1500个电话位置的记录。

在明尼苏达州，KSTP-TV 发现，从2018年到2019年，该州的地理围栏搜查增加了一倍多。大多数请求涉及非暴力犯罪。在纽约，曼哈顿地区检察官还使用反向地理定位搜查来获取反法西斯分子和极右翼组织 The Proud Boys 斗殴地点附近所有出现的电子设备的信息，以确定相关人员的身份。

谷歌在2019年收到了超过15.6万个政府索取用户信息的请求，但该公司没有细分出其中有多少是来自地理围栏搜查。

3、如何知道您自己是否已经被地理围栏搜查捕捞？

如果您的数据被收集并作为地理围栏搜查令的一部分交给了警察，谷歌应该通知你。

据美国全国广播公司新闻报道，对于许多无辜的人来说，这个通知可能是一个震惊，就像一个骑着自行车的人经过一个被盗的家庭门口。

但是，这些文件往往可以被封存或被禁言，这将阻止谷歌通知人们他们的数据已经被提供给了警方。警方声称这样做有时是为了防止正在进行的调查被揭露。

简单说，您可能无法知道自己的数据已经被警察拿走了。

4、警方有多容易获得这些搜查令？

您可能会认为一个横扫整个地区的搜查令很难获得。但是，有了地理围栏搜查这个名号，警方甚至都不需要一个嫌疑人的名字，就能让法官签字。

在2019年弗吉尼亚州警方的一个搜查令申请中，可能的原因包括“看到嫌疑人手里有一部手机”…… 几乎任何走在街上的人都拿着手机好吧 …… 结果是，仅仅因为这样，法官就批准了对该地区的全面搜查令，这使得谷歌交出了请求时间段内19人的手机定位数据。

来自明尼苏达州公共广播电台的一份报告发现，法官在短短4分钟内就签署了地理围栏搜查令，有时当局从来没有解释过有多少人将被卷入搜查、或区域有多大。

5、这些手令是否受到立法者的挑战？

联邦法律并没有禁止或限制这类搜查令，但州政府官员和律师正在质疑其合法性。

在纽约，州参议员 Zellnor Myrie 和 Dan Quart 在4月提出了一项禁

止地理定位搜查令的法案。如果能通过，这将是全国唯一一部阻止这种做法的法律。

“它不仅会禁止反向地理位置搜查，还会阻止官员规避搜查令，只需从数据经纪人那里购买这些信息”，监视技术监督项目的 Cahn 说。

全国刑事辩护律师协会也在弗吉尼亚州的一个案件中挑战了地理围栏搜查的合宪性。该组织认为，这种监视是违宪的，因为请求的范围太广。

国会就其 Sensorvault 数据库以及如何与第三方共享的问题提出了质疑，但是，没有具体解决地理围栏搜查令的问题。

6、这些数据会被误读或具有误导性吗？

由于这些搜查令上没有具体的个人或利益相关者的名字，因此，由此产生的调查往往会波及非常多无辜者。

当曼哈顿地区检察官办公室申请地理围栏搜查令时，谷歌给出了两个人的数据，结果发现他们是 Proud Boys 和 Antifa 斗殴事件发生地点附近的无辜旁观者。这两个人很幸运没有被捕，但并不是每个人都有这样的结局。

在时报的调查中，一名亚利桑那州的男子因涉嫌谋杀被捕，所谓的依据就是地理围栏搜查令 —— 他恰巧出现在杀人案事发地点附近。结果是，他在监狱里呆了一周，调查人员才找到了证明他无罪的证据。在此期间，他失去了工作，汽车也没了。

谷歌还在法庭文件中表示，提供的数据并不完全准确。 该公司表示，它估计的准确率为68%。

“因此，当谷歌被迫根据地理围栏请求返回数据时，有可能有些用户的位置估计在搜查令所描述的半径内 (其数据因此被包含在交给警察的范围内)，但实际上此人却在该范围之外”，谷歌在文件中说。

如果你只是使用谷歌地图寻找商店，这可能是一个小小的不便，但是，如果在刑事诉讼中使用这些错误的数据，那就是一个天大的冤案。

7、如何防止我的数据被这样收集？

简短的答案是，如果你要去参加抗议活动、或任何你不想被监视的情况下，请关闭手机位置服务，关闭您的Wi-Fi、蓝牙，设置为飞行模式。

但是有很多被地理围栏搜查令捕获的人，都是在从事一些没有什么理由认为自己会被监视的活动 —— 比如 去骑自行车出去玩，去银行，或者在自己的社区开车等等。

这些搜查请求也不只是向谷歌提出的。曼哈顿地区检察官的搜查令也发给了Lyft和Uber等公司。苹果收到的反向地理定位请求没有谷歌那么多，因为它存储位置数据的方式和Sensorvault不一样。

而即使警方不向谷歌或其他科技公司索取位置数据，他们也总能从数据经纪人那里购买到这些信息。这些数据经纪人搜集人们的移动信息声称追踪 COVID-19，但你要知道，这些数据也可以被警察用来追踪异议和反抗者。

数据经纪人从天气服务和手机游戏等看似无害的应用中获取位置数据，这个细节往往隐藏在通常不被人们阅读的隐私政策中。

今年2月，《华尔街日报》报道称，联邦机构已经转向位置数据经纪

人购买这些信息，而不是获得搜查令。Gizmodo 的一份报告概述了你的手机数据被广告商获取的方式，如何与你的身份挂钩，并提供给警方。

总之，除非您能练习在重要的外出中不带手机或者经常让设备处于飞行模式，否则永远会有被监视的风险。

[image]
[image]

您是否正在被 AirTag 跟踪？这里是检查方法

[image] 关键词	反追踪 定位
[image] 关联	定位追踪
[image] 创建时间	2025年10月5日
[image] **Description**	行动安全性

AirTag 被用来追踪他人，是一种越来越多见的恶意行为。您需要警惕。

[image]

在2021年推出 AirTag 时，苹果公司发布的这个带有超宽带的蓝牙追踪器被称赞为“向增强现实的未来迈出了一步”，“是寻找日常物品的好方法”，比如当你的电视遥控器找不到了的时候。但网络安全专家表示担心，这一跟踪设备会被恶意跟踪者所利用。如今 AirTag 已经推出一周年了，这些警告听起来愈发有先见之明。

模特儿布鲁克斯·纳德（Brooks Nader）说，在纽约市的一个晚上，一个 AirTag 被偷偷塞进了她的外套；在康涅狄格州，警方发现一名男子在受害者的汽车里放置了一个 AirTag，随后将其逮捕并指控其跟踪；多个州的警方已经就 AirTag 的潜在犯罪用途发出了警告。

下图是加拿大的故事。

[image]

较新的 AirPod 具有与 AirTag 类似的追踪能力，但苹果公司的耳塞成本较高，限制了其作为追踪设备的一次性使用。2月10日，苹果公司更新了 AirTag 的支持页面，提供了更多信息，并坚决谴责使用该设备追踪他人的行为。来自 9to5Mac 的报告显示，今年将进一步推出 AirTag 的更新。

尽管存在 Tile 和其他 AirTag 的竞争对手，但苹果生态系统的广阔性使该设备与众不同。如果你担心一个被秘密安置的 AirTag 可能正在记录你的位置，以下这些迹象可能有助于检测追踪器。

AirTag 正在追踪你的迹象

你拥有的智能手机类型会影响你发现隐藏的 AirTag 的容易程度。运行 iOS 14.5 或更新版本的 iPhone 手机的用户，只要有一个未知的 AirTag 在附近停留较长时间，就应该可以收到一个推送警报。苹果公司的网站没有提供触发这一警报的确切时间范围。

当你点击 iPhone 的警报时，可能会得到在 AirTag 上播放声音的选项，以帮助定位该设备。通过进入 “Find My” 应用程序，选择右下角的 “我” 选项卡，并确保 “物品安全警报” 那个按钮是绿色的，它位于 “通知” 下，以检查你是否会收到这些警报。

在 AirTag 发布几个月后，苹果为安卓手机推出了 Tracker Detect 应用程序。与 iPhone 的安全功能不同，这个安卓应用不会自动寻找未知的 AirTag。用户必须启动扫描。

据电子前沿基金会网络安全主任伊娃·加尔佩林说，该应用程序功能有限的原因很复杂。“这实际上是安卓生态系统如何运作以及安卓应用程序如何运作的一个限制”，她说，“我曾呼吁苹果和安卓合作，将苹果在iOS中提供的缓解措施水平纳入安卓操作系统，但这需要两个通常是竞争对手的团体之间进行大量合作。”

虽然一些寻找 AirTag 的指南建议使用蓝牙扫描器，但加尔佩林认为这种方法对于追踪器的搜索并不可靠。“我曾尝试使用各种蓝牙扫描

器以检测 AirTag，它们并不总是有效的”，她说。

依旧有很多人没有智能手机。如果手头没有设备，你必须依靠视觉和听觉的线索来寻找任何隐藏的 AirTag。这个白色圆盘比25美分略大点。据《纽约时报》报道，阿什利·埃斯特拉达(Ashley Estrada)发现她的车牌底下有一个 AirTag，她记录这一事件的视频在 TikTok 上被观看了2000多万次。

AirTag 刚发布时，如果离开主人超过三天，追踪器会发出响声。此后，苹果公司已经将这一时间缩短为24小时或更短。尽管有了这一更新，你可能也不想只依靠声音来检测 AirTag —— YouTube上的许多视频已经提供了禁用扬声器的DIY说明，无声版的追踪器甚至在Etsy上短暂上市。

如果我找到一个追踪器怎么办？

停用 AirTag 的最好方法是取出电池。翻转 AirTag，使有苹果标志的金属面朝向你。按住那个标志，逆时针旋转，现在就可以取下盖子，取出电池了。

苹果公司的 AirTag 支持页面建议，如果你认为自己处于危险境地，可以向警方求助。“如果你觉得你的安全受到威胁，请联系当地的执法部门，他们可以与苹果公司合作，要求提供与该物品有关的信息。你可能需要提供 AirTag、AirPods、Find My 的网络配件，以及设备的序列号。”

[image]
[image]

空中监视如何追踪抗议者？

[image] 关键词	反监视 空中监视
[image] 关联	🚁空中监视
[image] 创建时间	2025年10月7日
[image] **Description**	行动安全性

针对抗议活动的无人机使用并非只有监控一种，更有，携带武器的无人机镇压正在全球很多国家流行，而监视是一切镇压手段的基础—只有在维稳部队深刻了解抗议者的行动模式后，才可以采取非常准确的打击。

- Table of Contents

[image]

Unicorn Riot 团体获得了超过100个小时的红外监控录像，这些录像是警察侦察机在2016年公民社会组织 Standing Rock抵制达科他州输油管道的抗议活动中的监控录像。

执法机构使用无人机、飞机和直升机来监视抗议者，并跟踪任何车辆的行驶路径。看到视频：

几个月来，北达科他州公路巡逻队每天都在抗议者的营地进行监视飞行，并使用前视红外（**FLIR**）摄像机收集实时的地理空间情报（**GEOINT**）。

这些热成像仪可感应热源发出的红外辐射，从而使维稳部队即便在夜间也能精准监控地面活动。

> “我们确实是在打仗。”—— 卡斯县警长 Paul Laney 在国家警长协会网络研讨会上说，2017年5月7日（来源）

[image]

操作红外监视摄像头的警察经常会在人们不知情的情况下跟踪目标人的活动，这些无人机可以在漆黑的夜色中盘旋，监控地面数百英尺的范围。

[image]

在其他时候，侦察机被用来追踪抗议者的动向及其车辆。

[image]

在多种情况下，这种空中监视导致警察在拔枪的情况下将目标车辆拖到路边。

[image]

Standing Rock 反抗组织的任何人都可能会记得各种各样的飞机，这些飞机经常在头顶盘旋。

甚至在美国联邦航空局（FAA）颁布的“禁飞区”内，每一个白天到深夜，这些飞机、直升机和无人机，每时每刻都在盘旋。

[image] [image]

在抗议活动进行过程中的许多个晚上，都能观察到一架飞机绕着抗议者的营地盘旋数小时，而没有任何防撞安全灯亮着。

在地面上的抗议者迅速将其车辆的灯光射向天空，以寻找飞机，来自各个方向的光束照亮了天空。当飞机继续盘旋时，可能偶尔会看到光线从飞机的白色机身底部反射回来。

[image]

有时，抗议者会开始听到无人机在头顶潜伏的嗡嗡声，附近的每个人都会猜测那是否是警察的飞机。

根据 Unicorn Riot 组织获得的文件，大福克斯郡治安官已经部署了无人机来监视 #NoDAPL 抗议活动。这些无人机还配备红外监控摄像机。

[image]

> “没有第三次世界大战，我们就无法进入[那些抗议者的]营地。”—— 卡斯县警长 Paul Laney，国家警长协会网络研讨会，2017年5月7日（来源）

根据从联邦航空局收到的文件，大福克斯县警长在**D**、**E**和**G**级空域中使用了 **QUBE**、**Draganflyer X4-ES**、**X6** 和 **Phantom 4** 无人机系统（**UAS**）。

[image] [The documents also state that emergency law enforcement airspace requests would be coordinated through the Grand Forks AFB RAPCON, aka Air Force Base Radar Approach Control.]

当 Unicorn Riot 组织的记者要求大福克斯治安官提供视频录像时，他们拿出了一小部分带注释的图像和一些短视频。

这些数据显示是在无人机侦察飞行过程中捕获的，这表明警察正在收集抗议者营地、路障和管道施工现场的**GPS**位置。

[image] [Image take by the Grand Forks Sheriff’s Department during drone reconnaissance flight over Highway 1806 bridge.]

自从警察部门开始将其维稳设备军事化以来，在过去的几十年中，在全国范围内警察行动中，对IR监视技术的使用已经变得越来越普遍。

例如，海关和边境巡逻队也经常使用红外热成像仪追踪移民，并在美/墨边境沿线进行逮捕。该巡逻队也参与了对 **Standing Rock** 反抗运动的监视和驱逐。

到目前为止，维稳部门使用空中红外监已经有十多年的时间了。最著

名的行动包括，从2015年在巴尔的摩的弗雷迪·格雷（Freddie Gray）抗议期间、到2005年在纽约市举行的共和党全国代表大会，当时纽约警察局被指控侵犯公民隐私权。

Unicorn Riot 从100多个小时的FLIR监控视频中选取了两个小时的剪辑，您可以在下面观看：

请注意：针对抗议活动的无人机使用并非只有监控一种，更有，携带武器的无人机镇压正在全球很多国家流行，BACK https://iyouport.substack.com/p/0c8?utm_source=publication-search。

但监视是一切镇压手段的基础 —— 只有在维稳部队深刻了解抗议者的行动模式后，才可以采取非常准确的打击。

所以，活动家一定要警惕这点，尤其是需要日夜驻守阵地的抗议者，就如本文中介绍的这样。

[image]
[image]

当您准备参加抗议活动：基本指南

[image] 关键词	威胁响应 威胁模型 战略策划 抗议 街头 防御
[image] 关联	威胁知识库-索引页 ；行动安全性总述
[image] 创建时间	2025年10月10日
[image] **Description**	行动安全性

在参加抗议之前、期间和之后，如何保护自己的安全？

- Table of Contents

  在参加抗议之前
  1、在您的设备上启用全盘加密
  2、删除指纹解锁和 **FaceID**
  3、使用端对端加密
  4、备份您的数据
  5、购买预付费的一次性手机
  在抗议期间
  1、无需解锁设备即可拍摄照片和视频
  2、考虑骑自行车或走路去参加抗议
  2、启用飞行模式
  如果你在美国被捕
  如果你在中国被捕
  在抗议之后
  1、清除照片上的元数据
  2、如果您的设备被没收，该怎么办

[image]

在参加抗议之前、期间和之后，保护您的电子设备和数字资产，对于

保护您自己和您的信息安全、以及传达您的信息，至关重要。

盗窃、损坏、没收或强制删除信息，可能会破坏抗议的能力。与此同时，参与和平抗议的人可能会被搜查或逮捕，或者其他没有实际参加的人也会因各种原因被怀疑与行动者或团队有关。他们可能因此成为被监视和镇压的重点目标。

参加抗议活动存在风险，采取措施缓解这些风险可以在很大程度上确保您—— 以及您重视的数据—— 保持安全。

本指南概述了您可以在抗议之前、期间和之后采取的步骤，这些步骤将有助于最大限度地提高您的效率、并使您自己和您的数据更加安全。

请记住，这些提示是提高数据安全性的一般性建议，不构成法律建议或咨询。如果您有特定的法律问题，请寻求有执照的律师的建议。

[image]

返回：[image]S05街头实战指南-总章节：武器装备、组织协调 ... 全干货for激进社区晋升培训

在参加抗议之前

1、在您的设备上启用全盘加密

全盘加密可确保整个设备上的文件都经过加密。这是一种加密形式，可以保护静态数据，请不要与“传输中加密”相混淆，后者可以保护通过网络传输的数据。

全盘加密可以帮助保护从本地文本消息数据库到存储在浏览器中的密码的所有内容。如果您的设备被警方没收，或者丢失或被盗，那么全

盘加密可以帮助保护设备上存储的数据。

抗议情况通常是不可预测的，因此丢失手机是一种明显的可能性。

Android 和 iOS 长期以来一直需要将全盘加密功能内置到设备中。这些应受强密码保护：8–12个随机字符、易于记忆，并在您解锁设备时输入。如果设备不受强密码保护，则使用暴力攻击可以更容易破解加密。iPhone 5s 及更高版本具有专门的硬件来防御此类攻击，但复杂、强大的密码仍然是最佳做法。

请务必注意，仅加密设备可能无法加密外部存储介质，如 SD 或闪存卡。您必须单独加密这些，并且可能很难做到。您可能希望使用文件浏览应用程序调查文件在设备上的存储位置，或者从设备中删除外部存储媒体。

此外，许多数码相机缺乏加密能力。除非另有明确说明，否则必须假设使用数码相机拍摄的照片和视频将以未加密的方式存储。

2、删除指纹解锁和 FaceID

今天，iOS 和 Android 都允许用户使用指纹解锁（和解密）他们的设备，iPhone X 的 FaceID 允许用户使用面部识别进行同样的操作。虽然这些设置看起来很有吸引力，可以作为享受全盘加密优势的便捷方式，但是，启用这些设置意味着政府官员可以强制您用指纹或面部解锁设备。

在参加抗议的情况下尤其如此—— 或任何其他情况下，您可能会更容易遇到政府要求查看您的手机（如过境处）—— 我们强烈建议你把这个功能关闭。

在美国，使用生物识别技术（如面部扫描或指纹）来解锁手机会损害第五修正案提供给您的保护，该宪法有条款防止强迫入罪。

无论您使用生物识别码还是记忆密码，警察都可能会试图恐吓您“同意”解锁您的手机。但是，如果您行使拒绝权并且生物识别解锁功能已开启，则官员可能会强制您以生物识别方式解锁您的设备。

根据现行的美国法律，使用记忆密码通常会提供更强大的法律基础，以便在法庭上反对强制设备解锁/解密。虽然 EFF 继续反对执法部门强迫人们解密其设备的企图，但目前没有成功，

- 在 iOS 中，您可以通过进入设置 →触摸 ID 和密码（或设置 → 面部识别码和密码，具体取决于您的 iPhone 版本）并删除每个指纹，或点击此菜单中的重置面部ID来禁用此功能。

- 在 Android 中，禁用此功能可能取决于您的设备制造商。对于 Pixel 设备，请进入设置 → 安全性 → Pixel Imprint，然后从此菜单中删除指纹。

3、使用端对端加密

例如 Signal，是一款适用于 iOS 和 Android 的应用程序，可提供强大的加密功能，以保护短信和语音通话。这种类型的保护称为端到端加密，可保护您的传输通信。

除了加密一对一通信外，Signal 还支持加密群组聊天。消息还可以阅后即焚，在首次阅读后的10秒到一周内消失。与 SnapChat 等其他服务相比，这些短暂的消息永远不会存储在任何服务器上，并在消失后从您的设备中删除。

2016年，弗吉尼亚州东区的一个大陪审团向 Signal Whisper Systems 发出了传票，这是 Signal 的开发者。由于 Signal 的体系结构限制了存储在公司服务器上的用户元数据，因此他们能够提供的唯一数据是“用户使用 Signal 注册的日期和时间、以及用户与 Signal 服务的连接的最后日期。

在抗议的情况下，您可以将相关照片和视频发送给远程使用 Signal 的

朋友，这样如果您的手机被没收，您可以在以后检索到内容。

此外还有wire，并且不需要手机号注册，也推荐使用。

[image]

在本站工具-Tools 专题中搜索“IM”，以查找您可能需要的安全通信解决方案。请重点关注离线功能，因为活动现场被断网是很容易发生的事情。

4、备份您的数据

采取预防措施，以限制失去访问您的设备的潜在成本，无论是由执法部门没收的、还是丢失，或被盗的情况。定期备份您的数据并将该备份存储在安全的地方，以免您以后再担心。

5、购买预付费的一次性手机

大多数国家/地区都要求您提供一种身份证明形式来购买预付费 SIM 卡，从而将该卡与您的身份相关联，并消除匿名的可能性。

如果您担心保护设备上存储的数据，请不要带到抗议现场。相反，购买预付费手机。这些设备可以与大多数大型零售商店的 SIM 卡一起购买。

让你的朋友知道你的临时号码，并用它来协调活动。

请记住，移动设备的位置可以通过连接的手机信号塔来确定！因此，如果您不希望当局知道您的身份和位置，请在回家之前或可能泄露您身份的任何地方关闭预付费设备。

您的设备可能会存储您的坐标。出于这个原因，我们建议您关闭定位

服务。

[image]

延伸：https://iyouport.substack.com/p/wi-fi?utm_source=publication-search

延伸：https://iyouport.substack.com/p/wi-fi-bf4?utm_source=publication-search

请注意，如果您随身携带常规设备和预付费设备一起，那么这些设备的位置可能会相关并影响您的匿名性。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

在抗议期间

1、无需解锁设备即可拍摄照片和视频

抓住完美的图像是您想要做好准备的，而强大的图像可以帮助您实现目标。如果您选择了一个强密码，将其输入设备可能需要花费宝贵的时间来解锁，这样会影响您的抓拍。幸运的是，iOS 和 Android 都允许您在不解锁设备的情况下拍摄照片和视频。

这点也很重要，因为绝对不能为了方便抓拍而使用简单的密码或指纹识别。

2、考虑骑自行车或走路去参加抗议

自动车牌阅读器系统（ALPR）一直在自动记录驾车穿过一个区域的所有车牌，以及确切时间、日期和位置。这项技术经常被美国和许多其他国家的执法机构使用，或由 Vigilant 和 MVTrac 等私营公司采取，这些公司与执法机构和其他实体共享车牌数据。

这些数据被储存在大型数据库中，并且将保留一段未知的时间。这些公司已经游说和诉讼大力反对禁止私人收集车牌数据或以其他方式规范 ALPR 的法规。基本上，任何车辆的行驶历史记录都被随时捕获，对于如何收集、访问、共享和保留此数据的法律限制非常少。

> 如果您希望您的运动和组织保持私密，请考虑使用其他公共交通工具。在中国，切勿使用共享自行车、和不收现金的公交车、不要使用手机叫车应用程序、不要使用移动支付出租车费用。

[image]

返回：[image]自行车接力

2、启用飞行模式

飞行模式可确保您的设备在抗议期间不会传输数据，并阻止您的位置被跟踪。不幸的是，这也意味着您将无法向朋友发送消息或致电，因此请做出相应的计划。

在参加抗议之前，请在你和你的朋友可以见面的地方达成协议。你可能还需要关闭位置服务。

某些应用允许您在没有网络的情况下导航。启用飞行模式后，您可以选择性地打开 GPS。请务必事先下载抗议区域的地图。

如果你在美国被捕

如果您被警察拘留和询问，您有权要求在任何询问之前和期间与律师交谈。最好说“我想要我的律师，我选择保持沉默”，然后拒绝提问，直到你有机会与律师交谈。

但是，如果您决定放弃律师协助的权利并在没有律师在场的情况下回答问题，请务必说实话。向警察撒谎是一种犯罪行为，你可能会发现自己因为向执法部门撒谎而把事情变得更糟。

如果警方要求查看您的手机，您可以告诉他们您不同意搜查设备。他们可能仍然可以抢走你的手机并在以后用手令进行搜索，但至少很明显你没有允许他们这样做。

如果警方要求您提供密码来解锁您的电子设备（或要求您直接解锁），您可以拒绝并要求与您的律师联系。执法是否以及如何强迫您解锁您的设备仍然是一个悬而未决的法律问题; 向您的律师询问如何最好地维护您的第五修正案权利，以保护您免于被迫向政府提供自证其罪的证词。

您可能会因为拒绝提供密码或生物识别密钥警方将您的手机扣押。但是，每个逮捕情况都不同，您需要咨询律师，以帮助您了解自己的具体情况。

如果你在中国被捕

你最好不要被捕。如果万一被捕，记住，被讯问或调查谈话，最长只能24小时，要么出示拘留证把你送去看守所，要么放人。

记得：“法律要求你实话实说，但没有要求你说出所有的话”，所以你的口头禅应该是：“我记不得，记不清了”。

警察可能会向你宣读权利义务告知书，其中有两条：你可以聘请律师；你有无重大疾病。有病是非常棒的。

你需要主动要求请律师。在讯问笔录中都说“我要请律师”，这是写讯

问笔录的技巧。

查看并修改笔录，如果有任何不满意的地方，你都要拒绝在笔录上签字。

警察和颜悦色的时候也要记住那些人的体貌特征，高矮胖瘦，姓名等，万一被刑讯逼供可以在事后提供出具体的描述。

记住，你有拒绝上电视、上新闻的权利。

到看守所后，第一时间要求取保候审。要努力见到律师，律师会记录下你被带走的经过、留下的照片、伤情等。这些将成为法庭上的证据。

[image]

返回：审讯心理学

返回：[image]S07审讯心理学-总章节：不听、不信、不语，不放弃，不背叛

在抗议之后

1、清除照片上的元数据

准备好发布照片后，如果您不想泄露个人识别信息，最好擦除图像文件中包含的元数据。

照片上的元数据可以包括拍摄照片的相机型号，拍摄照片的确切时间和位置，甚至是您的姓名等信息。删除任何原始照片元数据的最简单方法是将照片传输到台式计算机上，然后截取图像的屏幕截图。然

后，您可以发布该屏幕截图而不是原始图像。

2、如果您的设备被没收，该怎么办

如果您的设备被没收，您可能有法律手段将其取回。在美国，如果您的财产在未决案件中没有作为证据被保留的必要，您的律师可以提出归还您财产的动议。如果警方认为您的电子设备上发现了“犯罪证据”，包括您的照片或录像，警方就可以将其作为证据。他们也可能试图让您放弃您的电子设备，但您可以在法庭上质疑此类资产没收。

您还可以撤消对设备上登录的某些服务的访问权限。

例如，在 Twitter 上如果您转到设置和隐私 →应用和设备，您可以撤销对有权连接到您的 Twitter 帐户的设备的访问权限。对于其他服务，只需更改密码即可提示应用程序注销。

但请注意，撤销执法访问权限或远程删除数据可能会使您面临被控妨碍司法或破坏证据的风险。在决定如何继续之前，您应该先咨询您的律师。

在线服务可能会为您的帐户提供最近登录的日志。如果您担心未经您的同意将您的设备用于访问帐户，那么查看此类日志是否可用并监控它们可能是必要的。

如果您的设备曾经被没收，又再次收回，请不要马上继续使用它！要警惕其中被安装了监视软件，关于如何应对这种状况：

[image]

返回：[image]恶意女仆和查抄

返回：[image]如果您的手机被盗了或被警察抢走了，怎么办

以上指南多次强调到律师的作用，以及您和可靠的朋友合作的作用，这非常重要。您需要在所处国家和地区联合到可以支持你的律师及同伴。

[image]
[image]

5种常用的“击落”无人机的方法

[image] 关键词	反击 大规模监视 无人机 空中监视
[image] 关联	[image]如何躲避无人机 - 监视时代须知 ；[image]空中监视如何追踪抗议者？ ；🚁空中监视
[image] 创建时间	2025年10月15日
[image] **Description**	行动安全性

1、信号干扰器：该设备也广泛应用于军事领域，其作用是通过干扰无线电波，破坏无人机对距离的监测，从而使其失去方向感。该设备采用2.4GHz频率（该频率对非专业操作者开放使用）；您可以在互联网上找到价格低廉的信号干扰器。部分无人机具备当主信号中断或无法接收时，强制返回基站的功能。

2、激光：使用激光笔，将激光对准无人机摄像头，其镜头/视觉传感器将被暂时失明或损坏。飞行员看到激光束时也很可能选择紧急降落无人机以避免其受损。

延伸：https://iyouport.substack.com/p/39a?utm_source=publication-search

3、**BB**枪/弹丸枪/气枪：当有物体进入无人机螺旋桨时，无人机容易失去平衡。所以一发精准的射击即可完成任务；不过需注意流弹可能造成的附带损害。

4、自杀式撞机：玩具/爱好者无人机售价约$100，而专业级无人机最

高可达$15,000。如果您持有很便宜的无人机，可通过强制与目标无人机发生空中碰撞，通过牺牲己方无人机的方法消灭监视者。最佳情况下双方无人机均会受损/或被摧毁，至少可使敌方无人机迫降直至空域安全。

5、钓鱼线/绳索：在两根柱子之间或建筑物的一部分与另一附近建筑物之间的高处位置（阳台或天台之间）固定一些线，以设置看不见的陷阱。飞行员很可能无法看到这些线，无人机会被挂住。

……

当然还有其他方法可以击落无人机，包括使用弹弓/弹射器以及其他发射石块的方法、或者拉网的方法。随时欢迎分享您的技能/知识和有效策略。我们可以一起增强抵抗力。

[image]
[image]

买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

[image] 关键词	一次性手机 移动设备 街头
[image] 关联	[image]匿名手机
[image] 创建时间	2025年10月16日
[image] Description	行动安全性

在中国，就算您只是出门和异议人士吃顿饭，也需要保持着参加敏感政治活动的安全意识和防御水平。

- Table of Contents

如何挑选一次性手机
使用密码管理器
设置和锁定诺基亚**1.3**或其他 **Android** 手机
关于匿名，您想需要注意什么
在参加抗议之前
在抗议期间
如果你被捕

[image]

任何一种给反抗者的建议都会包括这一条内容：不要携带您自己的手机去参加抗议活动。因为手机本身就是追踪器。

[image]

延伸：https://iyouport.substack.com/p/1200?utm_source=publication-search

无论您的抗议行为有多么和平，您都有被警察逮捕或殴打的危险。无需质疑，全世界的警察都不怎么讲理，只要他们声称“办案”，就可以做一切。

警察可能会没收您的手机并进行搜索 —— 所谓的数字取证，无论是否合法，或者他们可能会尝试破坏您的手机和电子设备，尤其是当您录制了包含当局暴力或非法行为的证据照片或视频时。

[image]

返回：[image]数字取证

[image]

持有证据的公民活动家需要特别小心这点。

同时，手机作为记录设备在抗议活动中是很有用的，可以帮助您及时传达抗议现场的信息。在BLM中有一个抗议活动现场的直播平台，来自多个城市。 这些资料来自街上的人。这是一种很棒的自发式公民社会协作，将有助于抵制官方的抹黑宣传，甚至有可能曝光当局的渗透（该直播已经离线）。

拍摄警察是完全合法的，并且在您的权利之内，它是公民打击警察暴行的少数工具之一。能够与他人实时交流或找到队友也很重要，以防您被疏散或围困。

为了平衡这种矛盾 —— 人身安全和联络+记录权的矛盾 —— 最安全的选择是将包含有关您的大量私人信息的主要手机留在家里，并携带专门准备的匿名的一次性备用手机参加抗议活动。

[image]

返回：行动安全性总述

那么，如果买不起/买不到一次性电话怎么办？Intercept 给了一些建议。

诺基亚1.3智能手机需要99美元，购买三个月的预付费服务还需要40美元。如果这对您来说太贵了，您可能还有其他选择：

如果您有老旧的手机还没扔掉，只要它仍然可以工作并且电池仍可以充电，就可以将其用作一次性备用电话，而不用购买新手机。

您只需要一张新的无关您身份的SIM卡。在准备抗议之前，请确保将手机恢复出厂设置。

如果您也没有老旧的手机，并且您决定带上自己的主要手机，请采取以下步骤以使其更安全 —— 私人数据最终落入警方手中的可能性较小：

1、禁用指纹和面部解锁功能，改为输入密码或口令来解锁手机。这样一来，解锁手机需要的时间就更长了，也大大增加了警察未经你同意就解锁手机的难度。

2、确保密码不容易被猜到。如果您使用的是数字密码，那么至少应该有6位数字，但越长越好。

3、设置**SIM**卡密码，这样可以防止警察从你的手机上取下SIM卡插入另一个手机，这样他们就可以接管你的电话号码。

这里是 iPhone 和 Android 的相关说明。如果您设置了SIM PIN，除了密码之外，每次重启手机时还需要输入SIM PIN。

如果您使用的是 Android，请确保手机的存储空间已加密（所有 iPhone 均默认加密）。在大多数 Android 手机上，您可以在“设置”应用中的“安全”>“加密手机” 下查找手机加密设置。

禁用所有不必要的智能手机功能，例如**Wi-Fi**、蓝牙和定位服务。您也可以在不需要使用网络时将手机保持在飞行模式。这将使您的手机泄漏的信息更少，那是那些警察可以用来跟踪您的信息。

如何挑选一次性手机

挑选一次性手机的主要标准是成本，这意味着 iPhone 肯定要淘汰。您也许能找到旧的或翻新的 iPhone，但 Android 手机可以很好地完成这项工作，而且花费要少得多。

低配的 Android 手机经常遇到永远无法解决的安全问题，因此下一个标准是寻找支持最新安全更新的手机。

Intercept 的记者选择了诺基亚1.3，在亚马逊上以99美元的价格买到的。这款手机于2020年3月发布，配备了最新版本的 Android系统，电池续航能力不错，相机也不错。

他选择的是 Mint Mobile。以40美元的价格在亚马逊上订购了带有3个月服务的SIM卡。

[image]

不论您最终选择哪种，其步骤都是近似的。以便宜为基本标准，以满足最低需求为目标。

使用密码管理器

密码管理器是数字安全的很好选择之一。它允许您使用强大的随机密码，而无需记忆它们。所有密码都被保存在一个加密的保险库中，你可以使用一个单一的口令来解锁它们，只需记住这个口令。

[image]

返回：[image]什么是凭据填充攻击？如何选择密码管理器？

一些不错的选择包括 Bitwarden、KeePassXC、LastPass 和 1Password。

设置备用手机时，您需要在密码管理器中保存以下信息：

- 预付费移动服务帐户的用户名和密码
- 一次性Google帐户的用户名和密码
- 用于解锁手机的PIN码
- signal的密码
- 与该手机有关的其他任何PIN或登录信息

设置和锁定诺基亚1.3或其他 Android 手机

观看他们的视频，以获取有关配置诺基亚1.3的完整教程，其中许多建议都适用于其他最新的 Android 手机。教程步骤包括：

- 插入预付的 Mint Mobile SIM 卡并激活手机服务
- 创建一次性 Google 帐户以与备用电话一起使用
- 安装系统更新，并调整所有 Android 设置，使其尽可能安全、并尽可能少的泄漏数据
- 安装和配置 **Signal** 应用，并在抗议期间将您需要的联系人添加到设备中，保证联系人信息不会被上传到所谓的云端

[image]

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

- 仅安装对您的联系和传播信息最有必要的社交媒体应用，其他都不要安装

- 备份您收集到的照片和视频资料，以防止警察抢走您的收集导致证据丢失，在这里看到方法🔙 https://iyouport.substack.com/p/5-f34?utm_source=publication-search

下图是在加利福尼亚州奥克兰举行的BLM抗议活动，使用这款一次性手机拍摄的照片效果。

[image]

关于匿名，您想需要注意什么

如果您随身携带手机 —— 任何智能手机，你的位置就没有隐私。警察能够使用被称为黄貂鱼的间谍设备（IMSI-catchers）来监控和收集抗议活动中所有手机的数据。此外，电信和技术公司也会从手机中收集自己庞大的位置数据，这类数据是不可能匿名的。

下图是追踪动图演示，在这里看到：

[image]

使用备用手机的时候，请仅在必须开机的情况下再打开电源、并尽可能令其处于飞行模式。这是最基本应该做到的。但如果您真的想确保你的备用手机与你的身份没有任何联系，您必须做更多的工作。

1、您必须亲自使用现金购买，而不是在线购买手机和手机服务，并选择可以让您激活服务而不要求提供身份证明的运营商。

[image]

返回：[image]匿名购买

2、每当您需要使用互联网时，都需要使用**Tor**浏览器、或远离你家和工作单位的公共场所的公共Wi-Fi网络。

3、绝对不要在同一时间里同时打开您的主手机和备用手机！也不要在家里打开那个备用手机！

除了数字安全之外，在抗议活动中您还需要采取额外的措施以保持匿名，比如：穿不显眼的衣服，遮住您的脸，遮住身体上任何纹身和疤痕，制定路线计划以避开车牌阅读器、不要使用可以追踪你的行动的公交车卡。

[image]

行动者从这里进入：自卫措施

在参加抗议之前

每次您准备去参加抗议活动时，都要清楚地知道自己要带什么东西。

除了您的一次性备用手机之外，把所有电子产品都留在家里。

不要带笔记本电脑、智能手表、或其他任何东西。

如果您打算用您的一次性手机带去参加不同的抗议活动，在您出发前往另一场抗议活动之前，一定要把一次性手机里的照片和视频复制到另一个设备上，然后删除手机中所有照片和视频，并删除之前抗议活动中的任何 **Signal** 对话。

结伴组团参加抗议活动是最好的选择。您应该把所有您认识的将参加抗议活动的人的电话号码放在您的一次性手机里，以备需要时可以联系他们。

如果您的朋友也带着自己的一次性手机，把他们的一次性手机号码放在您的通讯录里 —— 切记使用代号来标记这些号码！不要使用真名。

您也应该确保知道万一自己被逮捕了该找谁。

抗议组织者应该向与会者提供一个法律援助电话。您应该把这个电话号码用永久性记号笔写在你的皮肤上！如果你被逮捕，警察会没收你的手机，所以不要仅仅记录在手机上。

你会想在监狱里打这个号码的，以便获得法律支持。

在抗议期间

记住您的权利，不管警察怎么说，在公共场合拍摄他们是完全合法的。

拍摄警察是公民强迫他们为其行为负责的极少数有用工具之一。

在社交媒体上分享抗议活动的照片和视频是好事，但是，您也应该注意其他抗议者的意愿。虽然法律上允许你在公共集会中拍摄任何东西，但是，在拍摄人们的脸部照片之前，应先征得同意，这也是一种尊重。

您可能会因为担心被警察抢走手机而丢失了所有拍摄的抗议现场照片和视频，倾向于选择将这些文件上传到谷歌相册，以便万一警察强行删除了手机中的记录，记录也不会丢失。但是，不要忘了，谷歌相册是不加密的，如果警察和政府当局提出要求，谷歌就会出卖你。

如果你被捕

即使你是完全和平的，没有违反任何法律，警察也可能在抗议活动中逮捕你。如果您察觉到自己即将被逮捕，那么您应该迅速这样做：关闭你的手机电源。这样警察就很难进入你的手机了。

除非有搜查令，否则警察无权在未经你同意的情况下搜查你的手机。如果警察要求你解锁手机，或者抢走你的手机要求你解锁，请告诉他们，“我不同意被搜查手机”、“我拒绝被搜查手机。我需要和律师谈谈” —— 就算您还没有律师，也没关系，但是你必须明确说出这句话。

警察可能会没收你的手机，无论如何都会非法搜查你的手机，但是，此刻您最好明确表示您不同意，这样才能在今后有可能的起诉中避免警察反咬你。

警察也有可能试图偷走或砸烂你的手机，特别是如果他们注意到你拍摄了他们的暴力行为。如果发生任何这类情况，至少您能保证那只是您的廉价一次性手机，上面有最少的数据，而不是一个昂贵的手机，里面充满了关于你的私密生活和政治行动的敏感信息。

[image]
[image]

直接行动的关键在于协作，但协作的能力并非天生

[image] 关键词	关系 协作 团队 直接行动
[image] 关联	[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南S05E09 ；[image]S11关系结构革命-总章节
[image] 创建时间	2025年10月22日
[image] Description	行动安全性

人的一生中可能需要学习很多东西，但是，孤独和冷漠不需要学习，它是天生的；而协作的能力可不是天生的，协作不仅是一门学问，而且需要每个人克服很大的障碍以突破自己的 umwelt，才能实现 ……

- Table of Contents
应该如何工作
教育出了什么问题
更好的合作

[image]

挑战是生活中最随处可见的现实。人们一直在不断地处理需要他人投入的问题。民主就是一个协作协商的过程。

在现代世界中，人们面临着形形色色范围广泛、影响规模巨大的问题 —— 每时每刻都在尝试理解和识别与气候变化、网络安全、或专制政府有关的潜在解决方案。

但是人们通常并非天生就有协作解决问题的能力。实际上，关于团队的一个著名说法是：一群专家组成的团队并不构成“专家团队”。

[image]

协作是行动的基础。没有人能够是全能的，一项事业必需有各领域的良好协作才能完成。

令人不安的是，有证据表明，在大多数情况下，人们根本没有被传授过协作的技能。美国管理协会（American Management Association）在2012年进行的一项调查发现，高层管理人员认为，刚毕业的大学生都缺乏协作能力。

甚至更糟的是，大学毕业生似乎高估了自己的能力。2015年的一项调查发现，近三分之二的应届毕业生认为他们可以有效地在团队中工作，但只有三分之一的经理勉强同意这点。

悲剧性的讽刺是，一个人的能力越差，对自己能力的自我评估就越不准确。这个臭名昭著的达克效应也很容易发生在团队合作中。

也许不足为奇的是，在2015年对成千上万学生的国际评估中，只有不到10%的学生在最高水平的合作中表现出色。

而绝大多数学生无法克服团队合作障碍或难以解决冲突。

他们无法观测团队动态或采取必要的行动来确保团队成员根据其角色进行互动。

鉴于多年来所有这些学生都有在学校内外进行小组学习的机会，这表明在获取协作技能方面存在全球性缺陷。

那么如何解决这种不足呢？是什么让一支团队有效而另一支团队失败呢？

教育工作者如何改善协作式解决问题的培训和测试？

研究团队合作过程的专家提出了3点建议。

应该如何工作

在最一般的层面上，协作式问题解决要求团队成员建立并保持对他们所面临的情况以及已确定的任何相关问题要素的共同理解。

刚开始时，团队中的知识分配通常不均衡。成员必须保持沟通，以帮助彼此了解谁知道什么，以及彼此帮助解释问题的要素和应采用的专业知识。

[image]

返回：[image]是什么导致队友间不分享知识？

然后，团队可以开始工作，根据成员角色布置子任务，或者创建机制来协调成员行动。他们会批评可能的解决方案，以确定最合适的前进道路。

最后，在更高的层次上，协作式问题解决需要使团队保持组织化 ——例如，通过观测交互并相互提供反馈。

团队成员至少需要基本的人际交往能力，以帮助他们管理团队内部的关系（如鼓励参与）和沟通（如倾听和学习）。

更好的能力是能够采取他人的观点，以便考虑问题要素的替代观点。

无论是组织中的专业团队还是解决复杂的科学问题，清楚地沟通、管理冲突、了解团队中的角色、以及了解谁知道什么的能力和经验，都是与有效团队合作有关的协作技能。

教育出了什么问题

当如此多的学生不断参与小组项目或协作学习时，为什么他们学不到团队合作的技巧呢？

有一些相互关联的因素可能会导致人们协作能力很差却认为自己在团队合作方面相当出色。

由于普遍缺乏系统性的指导以及反馈不足的危险组合，令人们大大高估了自己的协作技能。

一方面，学生在高中和大学中会从事大量的团队工作。而另一方面，学生们很少会收到有关协作如何有意义的指导、建模和反馈。

数十年的教学研究表明，明确的指导和反馈对于掌握知识至关重要。

尽管实施协作解决问题的课程确实提供了一些指导和反馈，但不一定与团队合作有关。那些能迫使人们明确地反思自己与他人合作的能力的东西不存在。

更好的合作

现在我们已经确定了问题，那么该怎么办呢？百年的团队培训研究与数十年的课堂小组学习研究相结合，为未来指明了方向。

首先，最紧迫的是要在世界各地的教室中进行团队合作方面的培训。至少，这需要在大学本科教育期间发生，但更好的做法是从高中或更早开始。

作为反抗者，您可能无法指导教育体制，于是反抗组织负责人应该致力于在团队内部教授这方面的知识和技巧，并以身作则带动队友的协调能力。

这依旧需要组织者自己接受过专业的培训，并有意地在尝试过程中积累经验。

研究表明，协作能力是可以教授的，例如处理冲突和交流学习。研究人员和参与培训的工作者本身需要协作，才能将这些方法应用于课堂。

其次，人们需要有练习的机会。尽管大多数人已经有过团队工作的经验，但这需要超越书本理论。

实践中还需要学习跨学科的工作，因此可以实现跨专业解决复杂的社会问题。

第三，任何系统的指导和实践设置都需要包括反馈。这不仅仅是关于人们是否解决了问题或在学习课程内容方面是否做得很好的反馈。

相反，它需要有关推动成功协作的人际交往能力的反馈。

讲师应评估学习者的团队合作过程，例如 关系管理（鼓励彼此参与），以及在沟通上如何才能积极倾听队友的交流技巧。

更好的反馈是告诉人们如何才能很好地理解另一门学科的队友的观点。例如，工程专业的学生是否能够与法学专业的学生合作并理解新技术实施的法律后果？等等。

关于如何进行协作的明确指导、实践机会、以及有关协作过程的反馈将更好地帮助今天的人们做好准备，以共同解决明天的问题。

最后送您一首歌，Pentatonix 演绎的“ the sound of silence”。Pentatonix 团队也是协作的杰作之一 —— 这是关于种族、宗教信仰、性取向、性别、和政治立场皆不同的一群人，如何合作出优美的艺术作品。当您为合作难度过大而苦恼的时候，听听他们的歌曲吧，也许会有所启发。

https://youtu.be/gdVjVtpr55M

[image]
📌

纸条- Notes

二期工程“纸条”专栏中收纳的洞见大多来自本站首轮共创合作者，以及他们的地方伙伴。本项目一期工程中的同名专题旨在收纳理论/原理相关的见解；二期工程则欢迎更多闲聊和静思。

[image]

不是“个人问题”

[image] 关键词	关系结构 战术 等级制度 组织
[image] 关联	[image]S11关系结构革命-总章节
[image] 创建时间	2024年9月18日
[image] Description	纸条

[image] [image] [image]

如上图，所有这些选项也许都存在，但它们都不是根本性原因。

您可能也经常奇怪于某些人为什么这样做或那样。但如果把这些现象归因于个人问题，那就会错过很重要的东西。人的行为方式基本都是伴随其成长过程的制度的产物，而不是“天性”。

[image]

制度性越强天性就越弱。越近距离的关系，对人的影响就越强。

换句话说，是社会关系形成了个体而不是反过来。

如果只是把集体拆开还原成个体，并不会帮你弄懂个体，也不会弄懂集体。

因为集体不仅包含个体，更重要的是还包含个体之间的关系，是这种关系结构在对集体中的个体产生影响。

掌握权力的人通过剥夺其他人的权力而产生。通过对身体的胁迫、对

经济的支配、以及对心理层面的限制的总和，社会制度和惯例影响着其中的每个人对自己的地位和对整个世界的观察方式。

专制主义就是一种社会关系，它把社会分为少数的统治者和多数的被统治者，导致后者的普遍贫困 - 这种贫困不仅仅是经济问题，更有精神、情感、欲望等等所有方面的被亏欠。

在这种社会关系中，人际关系的烙印是权力，而不是自由。于是在这里，一切都是基于权力的，这种社会关系不会也不可能自由地教育人。

[image]

只有对生活的各个方面直接参与 - 自我管理，即自主 - 才能自由地教育人。

异议人士社区/团队如果不能从自身组织的关系结构层面反叛专制主义 —— 如果你们之间也保留着等级制度、吹捧和压制、竞争和虚伪 —— 就只会根本性地失败。

这里的失败从立场层面开始，意味着该群体只是在复制它本该反叛的系统，所以它已经不能被称为反对派。

包括论坛在内的等等都属于项目，这些项目可以是行动也可能是运动的一部分。但只能是先有组织后有项目；如果一个组织的人际关系结构只是专制体制的复制品，它形成的任何项目的受益人都将是专制体制本身。

中国朋友喜欢说的“体制内/外”，如果指的仅仅是职业和福利待遇区别，那就太窄了。我们认为“体制内”应该指的是在任何方面复制和帮助延续系统特征的行为。“体制外”则相反，应该是变革的尝试者。

[image]
🍻

你在人际关系处理方面遇到过哪些尬事？贴张便签，我们聊聊

[image] 关键词	人际安全 关系 团队 威胁识别
[image] 关联	🎀人际安全&关系结构革命-RelationshipsRevolution
[image] 创建时间	2025年1月1日
[image] **Description**	纸条

IYP：强调大原则 —— 切勿谈论任何具体的人和组织名称；违者将被删除留言，不做单独解释。

[image]

在没有清晰的、共同战略的情况下，“聊天”只是情绪口水而已。比如我的经历，不少后来我自己实现了的东西，其实其构想，在之前很久就在圈子里说起过，有的还说过多次。但没有任何人鸟我。倒也好，这让我有机会亲手实现了这些想法，尽管毫无疑问遗憾的是，其中不少东西如果有协作的话，其结果显然可以更大更深远。

[image]

我曾经加入过一个写作团队。有点类似iyp的共创，大家在同一战略下写作，解决彼此显见的问题，然后分享以帮助更多的人。大家使用同一个名字。没有任何人能支配其他人。每个人都想着如何更好的解决问题。在这个过程中我学到了非常多的东西，对我未来的发展大有助益。可惜我们不是“知识分子”，我们不追求独家理论和专著，也不会扬名天下，我们只想解决身边最棘手的问题，化解障碍让事情更顺利。真的希望知识分子们能更多加入这样的合作。他们显然是一些更聪明更博学的人。

[image]

我觉得我基本可以肯定不会跟老自由派异议圈子里的人谈恋爱。我想我可能永远无法忍受那种把人当成工具的交易心理。开始都不要开始，注定会失败。而一旦失败，他们就会用人格暗杀来给自己挽回面子 - 说你是间谍、渗透者、玷污你所有成绩，毁掉你的公信力。

[image]

我离开过一个团体。尽管我没有离开运动。但我后来一直在忐忑。这个团体使用大陆异议中比较流行的话语，尤其是“冲塔”，并对镜头感 - 而不是战略效用 - 持有令我胆寒的追求：认为行动者必需被捕才能“被看到”，只有被看到才能“有价值”。

我觉得事情被完全搞反了。我担心自己万一一直都不被抓，会不会被鄙视，甚至被怀疑 …… 我很怕。怕身边人胜过怕条子。我知道事情错了。我在它变得更错之前离开了。

[image]

能帮就帮一把。甭问需不需要。

我需要什么？我需要活下去的力气。

也许一个36摄氏度的拥抱就能让我有力气再活三十年，但如果你问我需要啥，答案永远都是：什么都不需要。

乞讨到的东西实现不了革命。

[image]

不要和自由派异议圈子里任何人交往。你只会被一味的索取，从人际资源到性资源，等你被剥干净了后就会被毫不犹豫地扔掉 —— 不要误会这并没有任何针对性，所有人类在市场资本主义者眼里都是货品。

[image]

当我什么都不怕了的时候，却是把自己吓到了。 因为我整个人变得虚空了，欲望被抽离了身体，像云朵一样漂浮在远方的天空中，能看到，但摸不到，也不再能影响我。

[image]

“人脉资源”、“社交资本” … 这些词语听起来都很危险。你很努力地在各种圈子里扮演老好人中央空调，以为自己在积累所谓的社交资本，而最终这份“资本”你根本无法使用 —— 你越是“高资”就越是如此 —— 唯一能使用它的人是条子！

换句话说，你一直在努力“搞人脉”而不是搞志业的辛勤，事实上只是在把自己不断推向被条子要挟做线人的死胡同。

如果你被拉近一个江湖文化的圈子、你发现其中的人们对人脉资产的重视程度远高于其他（政治理想只是人设而非凝聚力），不论那些人嘴上宣称的立场听起来多么“进步”，赶紧跑吧，跑快点别回头。

[image]

想象一下，一个自称激进的圈子里最具指导性的文化是：认真你的就输了。

[image]

其实我很难理解，为什么某些自称“激进”的圈子居然能容忍对政治一窍不通的成员，并不是观点问题啊，是那种纯粹的政治无知，纯属不理解激进战略 —— 如果一个人连“为什么加入这一阵营”都搞不清楚TA加入的目的是什么？而且还在圈子内处于多种层面的指挥控制地位，目的是什么？如果一个人连事情错在哪里都无法完全了解、唯一擅长的只是人云亦云，何谈抵抗？靠人脉资产社会地位作为筹码的交往规则真的不要自诩激进了。

[image]

一边声称追求“自由爱”，另一边是玩腻了就甩，老婆只是个工具，被用来在甩不掉被玩弄对象的情况下搬出来维稳。没老婆的就用屎盆子替代——玩腻了想甩的时候就说对方是“燕

子”、“非常可疑”。这种帽子扣在任何人头上（甭管男女）其政治生涯基本就终结了。

最初只是对解放性的关系结构的浅尝，最终调动出了这些人被内化的党国“式”镇压神经元。这些自称“自由主义者”的人就此暴露出“自残主义者”的本质。

抱歉我说的太狠了。但绝无恶意。一切只是失望。因为曾经抱着巨大的期待、怀揣着“实现一个截然不同的崭新世界”的梦想加入到这一群体中的，这份失望足以致命。

[image]

我收到的鸡鸡照片比我真正认识的“异议人士”都多。我一直都没想好能用什么更准确的措辞来形容这种啼笑皆非的圈子潜规则。其实也不需要说什么了。

总之我已经没心情认识更多这些人了。

[image]

圈子里的蟑螂和厕所里的那些截然不同。前者相当会讨喜、人脉资产丰厚，甚至能得到所有人的支持；而恰恰是这类人，一反手就能把所有人带进深渊。

那些依赖口头赞许如生命线般紧要的嘴炮异议们对圈子蟑螂的陷阱毫无抵抗力。

[image]

拒绝所有完全无关爱的关系邀请。每一种，不论任何名目。不要问我为什么。祝福你永远不必了解为什么。

[image]

一起看电影吧。比一起看书或者读书会的效率更显著，反正我的经验是如此。如果你身边有个特别懂电影语言的亲密朋友，

尤其是领悟力特别强的那种人，那感觉真的很棒。你会发现很多自己看的时候错过了的深刻元素和细节。

[image]

不要信别人告诉你如何亲密。谁说的都别信。不要轻敌，也不要被那些失败者的抱怨吓倒。

自己去试试，自己摸索。

相信我，你最终会得到比他们所有人都好的东西。

[image]

给大家多点机会实践吧。我还是那话，我们的解放世界只在梦里出现过少许片段，想要在现实中复制出来我们就需要特别多的试错勇气和耐心，耐心比勇气还重要，心急会吓跑勇气。

我当然不是说主张容忍所有错误，有些错误就是背叛革命的，对那种情况不能妥协，但很多时候，互相体谅一点点没有坏处。

[image]

我们中很多人太缺少鼓励了，缺少认同，隐性的竞争比鱿鱼式决斗更残忍，因为你不仅要躲还要猜刀子在哪。我们这些精疲力尽的人聚在一起就是想要互相安慰一下，讨点情绪价值，所以你会看到比较搞笑的（准确说应该是很心酸的）状况—— 我们互相吹捧，互相点“在看”，互相转发，我们的“思想”（如果有的话/其实更多时候只是唠叨而已）只能在自家圈子内部和周边兜兜转转。我们以为自己很孤立，事实上很多时候我们只是在用各种方式自我封闭。

这种情况下大家都不敢尝试新东西，因为仅存的一点点“被看到”的安全感完全来自周围人的“熟知”，人倒了人设也不能倒。

尤其异议圈子，你的思路一旦变化，甚至容易被怀疑成叛徒/线人卧底 —— 你别笑因为绝大多数人都压根不懂怎么判断卧底，更甭说处理了，加上害怕、更有竞争心态和等级制下的焦虑，瞎扣帽子是常事。

为什么我们不能培养一些鼓励创造性和建设性洞察的圈子文化呢，如果我们彼此间足够分享情绪价值，也许能促成更多变革热情呢？

我觉得应该是这样啊。

[image]

“无用”是一种勇气。在这个鱿鱼世界里，敢于让自己无用、无力，无能，一无是处，是一种极大的勇气。卸下所有强加给你的要求和期许，作为一个生命体，去感受被珍惜、被理解、被尊重的权利。

给自己一份“无用”的勇气。你将能够筛选出真正值得你珍惜的关系。

[image]

自大是灾难性的。每个人都自大是相当灾难性的。导致真正用心关注你研究你的人了解你的一多半人都是你的敌人。光想想都让人胆寒。

这是自由派中产阶级圈子的根本性失败因素之一。党国比他们的潜在盟友更了解他们的一切。我见过很多这种情况。很悲剧。

[image]

不米兔那个系列看得五味杂陈。

只要有等级的地方，就永远不可能有正义，人们会为了面子和

地位攀爬机械性地讨好高高在上的圈子大佬，几乎没有人敢站出来主持公道。即便每个人心里都明白你说的对、你是委屈的、你在背黑锅，但没人敢为你站出来，因为你是个边缘户，不值得为你耗损社交资产。

[image]

“合群”这个词已经基本变成纯粹的贬义了。这就是对巴结攀附潜规则的反叛。

[image]

每一个情爱演变为冲突的案例都属于安全事故；造成事故的原因从根本上说都与信任不足有关，信任不足导致团结破裂。

团结起来就能抵抗这个垃圾世界，就不会出现这类事故，团结的基础是信任，持续稳定坚固的信任只有爱能做到。所以，简单成一句话就是，安全事故是错失爱导致的。爱是最强的安全措施。

米兔相比下只是个小例子。异议圈子最广泛的反动和无能的本质就是爱无能。如果你无法爱，你就无法合作，如果你只会博弈，就难以互信，没有互信就无法联合，就很容易被渗透。博弈的关系结构是蜂窝状的，千疮百孔，任何一个方向的侵入都可能瓦解它。

相反，如果你想要安全，那就必须合作，必需联合起来共同抵抗。这只有爱能做到。

[image]

信誉是需要某种测试的。合作的风险越高就越是如此。测试方法很简单，告诉对方一些看起来很像是内心深处最隐晦的秘密的东西，并叮嘱其绝对保密，然后等着就行了。等着看会被泄漏多少。选零泄漏者合作。保密原则是人品的唯一体现。甚至政治观念都是次要的。性偏好神马的就更不值一提了。如果你发现某些圈子采用非原则性的古怪的价值观评判他人，远离那

些人，他们早晚用同样的价值观评判你。在草木皆兵的人际关系中被扣屎盆子是天下最恐怖的事了。

[image]

在你开始之前你必须接受一件事：没有任何人会心疼你的付出，没有任何人会理解你的艰辛，你将遭遇到的除了镇压机器外只有摘桃子、吃瓜、人血馒头。

刚那位朋友说的“除非被抓否则不会被看到” 那就是事实。不客气的说几乎没有人会相信你的反抗“不是为了移民庇护”。

你得接受所有这些事。接受一切。嚼碎，吞下肚。然后，如果你觉得依然有必要继续反抗，那就去做吧！那个时候你才是无敌的。

[image]

很多人都不是被党国的镇压黑手吓跑的。而是被反贼圈子里的肮脏吓跑的。他们看不到希望了，只能选择维护自己最后一点尊严，隐退了。我们本该有很多有能力的战友足够撑起一片天，但他们太孤独了，因孤独而疲惫不堪，最终放手。这是我们所有人的失败。

[image]

男人无能的时候就只会用性来羞辱你。
只有最无能的男人才觉得性是可以羞辱女人的东西。
当有人用性羞辱你的时候，你就知道你已经全面碾压他了。

[image]

我们最□的担忧之□就是异化。
“颠覆□常□活”对我们来说不仅仅是□句□号。它是我们存在的根本。
当前的社会关系陷□了买卖、交易、以及由此产□的狭隘“□份”和永无止境的冲突分歧的庞大空虚之中。我们许多□发现□□□处的所谓反□化将可能永远是资本可以从中收获的市场。

所以，我们不需要亚□化及其壮观的时尚、规范的□为和各种商品的深奥知识。我们希望在所有这些该死的营销吹捧和消费操纵之外重新建□以“人”为基础的联系。

[image]

受害者，反抗者，和革命者，是三种不同的人。

- 受害者哭诉，目的是让更多人了解自己的遭遇，其过程将导致加重自身独特性/自我边缘。

- 反抗者对峙，以牙还牙以暴制暴，结果可能导致噩梦反复不断。

- 革命者则旨在创造一个新的结构取代现有结构，从而终结灾难，实现解放。

[image]

很多自称左派的男性从不反思自己的厌女倾向，因为他们认为自己与女权主义走得近（请注意仅仅是走得近而不是参与）就能让他们免受父权制的束缚。所以这种人往往是最糟糕的、最会操控女性的伴侣。

相比下保守派男性是真小人，公开仇恨女性毫不掩饰，每句话都臭气熏天能噎死几个。该吓跑的早都吓跑了。

但那种表面上尊重仅仅因为你的政治立场与他一致，而实际上却始终要踩在你头上的阴险仇恨的伪君子，简直令人发指。我自己就经历过，我认识的几乎每个女性都经历过。

[image]

Waiting for you!

[image]

当你感到被孤立的时候，你就容易要么孤注一掷，要么畏缩不前。

[image]

我拉黑某人并不是因为他在跟我约炮。而是他的姿态。压迫性的高高在上的姿态 —— 他似乎是在指出我有“义务”提供性服务，同时也在强调他有“资格”要求我提供性服务。这也是该圈子的普遍共识，即将人视为资产，于是交际便被视为资产交易。这是比性别歧视更糟糕的对人格尊严的歧视和操弄。

[image]

如果他们无法控制你，就会拉帮结派地孤立你。

[image]

被“自己人”毁掉的可能性，比被敌人毁掉的可能性，还要大，这是顶级的灾难 —— 只要人们还在等级制度中相处、在竞争结构中互动，就没有人能逃离这一顶级灾难。

[image]

你知道吗，被爱笼罩 - 而不是被焦虑笼罩，被爱驱动 - 而不是被仇恨驱动，那种感觉真的是太棒了，好幸福，好振奋。如果人生真的有“巅峰”，那一定是某种领悟带来的升级时刻。这才是我们这些站起来反抗的人真正追求的东西。你一定要知道，这份美妙，你也能拥有。

[image]

清迈的事情时，有一位关系很近的朋友很严肃地问我："到底是反贼赚得多还是顺贼赚得多？……到底跟着谁能过好日子？"
我陷入了沉默。
我一直以为，反叛就是自我治愈的方法，赚再多也不会实现的深层治愈。我以为这是众人皆知的。但现在我发现，也许并不是。

[image]

我如今几乎所有时候都只是说"我明白"。而不是说"你说的对"或者"不对"。

我不需要评论你的话，不论你说什么，但你可以放心，我一直在努力去理解你 —— 我理解你的沮丧，你的哀怨，你充满委屈的失落感，我都明白，明白你的爆裂情绪从何而来。

希望我泪光闪闪的眼神能帮你照亮一条前行的路。

[image]

你们这些小屁孩太放肆了，你知道我是谁吗？连A某（公认的圈子领袖之一）都要敬我三分……做人得识时务，懂不？……

—— 这是一个圈内大佬在跟我约

炮并被我拒绝后对我说的话，用吼叫的方式说出来的。我很庆幸那之后他就拉黑我了。

[image]

女人不能能力太强，否则就会被说成是燕子。必需至少能被圈子里高社交资本的男人完全控制，否则根本无法在圈子里立足。我个人不觉得这样的圈子值得我维护，不论他们宣称什么样的政治。

[image]

我是从“心理安全”部分加入这个项目的。可以说深受触动。

想象一下，当你亲眼看见亲耳听见你信仰了多年的异议大佬、甚至可以说就是你的革命精神支柱，在你和其他一些人面前吹嘘自己“最新操到的年轻姑娘多嫩多水”，你整个价值体系都会被摧毁，那种贪婪猥琐的表情会在你每一场噩梦中浮现。

有人问我为什么离开那些人、为什么不参与讨论，我没有真正解释这些，我只是觉得这些人很可能永远无法实现他们声称追求的世界，因为旧体制的所有垃圾已经完全驾驭了他们每个人的中枢神经系统，他们已经变得和统治者没有区别了。

[image]

女人不要留在这类圈子里。我很严肃的说这话。反正我爱的女人我肯定不会让她进入这类圈子。在这

里，如果你不幸年轻又漂亮，你只会被轮番玩弄然后给你扣一个“婊子烂货”甚至“燕子”的标签再扔掉；如果你年老色衰，除非家庭背景能达到让那些人跪拜的等级，否则根本就没人愿意多看你一眼，你说任何话都不会被听到。

我是直男，我看不出某些圈子的颠覆能力，在我看来他们的风格跟党国没有任何区别。

魔鬼的反对者不都是天使。也有可能是魔鬼**2.0**版。

[image]

我说句公道话吧。为那些你们嘴里的直男癌说句话。我也曾经是其中一员，尽管现在不是了，但当时的心境记忆犹新 —— 所以现在我可以实话告诉你，圈子文化问题巨大，虽然自称异议但始终没能摆脱统治系统的价值体系的结果。

在这种情况下你在圈子内混和在社会上混并无本质区别，所有垃圾体验一模一样，这正是为什么其中绝大多数人张嘴就吹嘘自己操了多少良家妇女，因为不这么吹的人只会被视为“不行”、“没有魅力”、“水平太低”、“社会资本太差”。

你觉得那些看起来老色批一样的家伙都是只会下半身思考的畜生吗，都不理解爱的意义、都不想要一个安稳自在的亲密关系？不是的。

诚实的说没有人不想要。

但确实有不少人觉得自己要不起。

他们嘴上反对在位的皇权，但心里对未来一筹莫展，扮演老色批、吹嘘性资源 - 换句话说压迫更弱的人 - 对他们来说是为数不多的/甚至仅剩的成就感来源，成就感是生命意义的支柱啊，你懂吗。

我绝对不是说老色批人设有任何正当性，事实上嘴上长蛆的那些家伙现实中也没骚成那样，他们只是好失落，加上政治想象力特别特别差几乎为零，他们想象不出国家政府的男权系统之外还有任何其他可能性。更妄谈尝试。

[image]

倾囊买进谷歌阿里股票的人也能自称“反监视”，就如在军工股上赚到飞起的人也能自称“反战”“热爱生命”，动动手指操弄几只股票、几条“热搜”新闻就能把那些自由派中产一网打尽。

请记住这点。这是我们共同的深渊，也是我们必须正视的变革起点。

[image]

体验一下。当你正焦虑不安手足无措的时候，在YouTube给自己选了

一只冥想音乐准备坐下来自我疗愈一下，你刚进入状态一点点，忽然间，音乐停了，插播进一条广告！你还关不掉它，除非你马上掏钱（社会资本和潜规则/导致你焦虑不安的根本）……

就像一块巨石砸在胸口上。广告过后的音乐声犹如噪音。你再也回不去最初的状态了。

这就是自由派改良主义圈子带给很多人的感受 —— 不只有一块接一块的胸口大石，还有绵长的失望和恐惧，我代表离开的人说声抱歉，可能短时间内没有力气加入任何新的阵营。

除非…我们能亲见一些真正的改变。

[image]

刚那位朋友提起的问题我可以回答：关于“如何判断是否自由派鱿鱼圈子结构”。

鱿鱼结构有一个典型的标志就是，越是看起来“亲近”就越是无法深度探讨严肃问题、动员力反而越差。这是因为交往是交易性的，交往的方式是各方都在竭力展示自己的“可利用价值”，生怕自己看起来“不够优雅”、“得罪人”。在这种情况下你不可能体验到那种灵魂碰撞的深度连接。

注意力都在自己身上的结果还会导致对周围人的了解严重不足。由于没有深度探讨、没有思想磨合，一个人多年前早已达成的领悟很难对旁人产生影响，甚至不为旁人所知，越是看起来“亲近”，就越是如此“陌生”。

[image]

要跟“人”交往，而不是跟人设交往。亲近真实的人，而不是各种光彩夺目的身份标签堆砌起来的广告牌。

如果全世界能有千万分之一的人做到这点，或者百万分之一的人想要这样做，变革便已到来。

[image]

我想寻求答案。事情就不能简单一些吗？

严格的保密政策让我们中哪怕是最亲密的关系间也难以完全轻松地倾心相处，这种心理压力，长此以往会伤害我们所有人。是的我们可能没有被条子连锅端，一定程度上这让我们暂时免于镇压的威胁了，但我们的代价包括难以避免的心理损伤成本 ……如何才能平衡它？

[image]

脱离所有吸血的关系。至关重要。

什么是吸血？如果对方跟你在一起一直都只是想要得到你的关注和赞许，却从来无视更不会考虑你的任何遭遇和任何时候的艰难，那就是拿你当血包了。长远看这样的关系真的只有消耗。

[image]

在招募工作中，人格魅力是一种极为方便的工具。

但如果你完全依赖人格魅力构建凝聚力，你将只能得到一个饭圈，而不是一大群同志。

[image]

我是参加你们那个创伤康复训练的。最让我惊讶的是，我忽然发现我以前百思不得其解的问题、让我痛不欲生的很多困境，其实前人早就经历过了，一模一样的状况，早就有解了，我自己关上门孤独地发明轮子并没超出前人半分。

世界各地的反贼前辈的经验都不在寻常的书里视频里，很难找，没法流通，不光我，我觉得多数人都不了解这些。希望IYP将来多组织这类活动，真的很不错。

我这条不是社交尬事，是我觉得我们的社交远不够充分。

[image]

你必须去爱一件东西，任何东西，什么物种都行，是不是生命都行，有形无形都行，要有至少一个这样的东西，能让你去爱，必须去爱，发自内心地全神贯注的去爱这样东西，让它安放你的心，只有这样你才能在这个凶残的世界里活下来。

[image]

战略共识虽然没有，但却有个基本共识，就是，大家都默认其他人和自己不在一个战壕里，于是全都彼此留一手。各种对话中都能感受到这点。你带着真心来了，结果却是，超尬。

[image]

对任何关系来说都是如此：你们之间“不能说的话”越多，你们的关系就越差。不论这一“关系”中有多少人 - 2个人，500人，还是九千八百万人，或者14亿人 ……

不存在0界限的关系；但界限过大时，就不存在“关系”了。

团结不是用嘴喊出来的。团结是同在一个结构中的人们的共同认识和需求。当你看到人们在想要讲述些什么的时候先强调立场，而不是先摆事实，以避免自己被同伴误解为“异端”，这意味着出了大问题。某些圈子/团体的这种文革式极化导致了很多失败。

[image]

隐藏的严重问题在于，一些人的价值观 乃至价值体系 都是非常短视和自私的。比如 最常见的，把阅读和交流当作混圈子的资本，这个错误的目标导致他们不再学习 而是倾向于模仿，或者用他人表面上的意见一致 来证明他们自己的想法是正确的，然后再把模仿到的和证明到的东西“转卖“到别处。

整个过程不产生实际价值。它只是通过微调等级关系巩固了等级制度。在这种结构中 表面上看起来有可能我们的观点得到了主动的传播，但由于传播者的价值观不促进合作，结果很可能与我们的目标相悖。并且 随时都可能有更能扯蛋的人把这些人的意识抢走，因为他们的目标就是扯蛋，在扯蛋中竞争取胜，而不是共同进步和合作。

做个实验就能简单测试出来，我几天内不提供私人见解，一个自称左的人就开始发表很右的观点，显然是受其他人影响了。这类都不行。而社交媒体的奖赏机制一直在培养这种人。

[image]

跟一个哥们聊到深夜。罕见的亲密交流。他家直系亲属里有4个警察…… 按理说我应该直接给他一闷棍对吧？并没有。因为他在讲述这件事的时候，流露出的是一种归属的安逸感，甚至包含着自豪感也是完全是归属满足带来的，而不是对权力/武力/暴力的掌控所带来

—— 用他的话说就是，对于“被看见”、“被待见”、“被认可”并有机会展示一技之长的感恩。他掩盖了很多东西是的，等级制的压力、官僚主义、屈从的辛苦等等一切，他都没有提起。

但他流露的感激之请令我心酸。因为，我想到的是，我们的圈子/社群什么时候才能让投靠我们的人在陌生人面前如此般洋洋得意地夸赞自己的归属满足感？那个时候，就是我们能战胜这个统治机器的时候。

[image]

从根本上说，是博弈的结构让反馈始终缺少建设性。与性别无关。甚至多数时候，人们都很难从反馈中获得能量（认同、赞美、鼓励、仰慕等等都可以积累能量，绝不是吹捧哦）。

这就要求一个人不断证实自己，不证实即证伪。

这就是制造睡粉现象的机制。男性寄希望于用性入侵的方法来加强崇拜的稳定性，以“证明”自己。不是发泄，更多是占有。当然更与情爱毫无关系，它在等级的基础之上，或者准确说，就是由等级制导致的，它本身就是一种压迫。

博弈结构必需反情爱。因为只有在取消所有等级的情况下才能有情

爱，一旦情爱，博弈的结构就崩塌了。

米兔声称捍卫的东西本应是旨在反击这种压迫，然，归因偏误导致它最终变成了规训。规训是对自由的剥夺。剥夺自由者是统治的盟友。由此，它就叛变了。

整个问题一直无从解决的原因，恰恰由于缺少了最重要的一份力量的联合 - 就是被米兔变成敌人的那些人。

……至于如何做，详见本站相关教程。

[image]

努力给彼此以荣耀。让身边的人知道TA留在这个群体里、留在你身边，是正确的选择。作为反叛者我们没有社会地位那种庸俗的荣耀感，甚至都可能没有公共社会网络中的存在感，我们唯一的依靠只有我们彼此的肩膀。我们的肩膀必须是坚实的。我们绝不是普通的“抱团取暖”，而是要真正地结合在一起，共同创造，共同成长。

这件事在中国也至关重要。一方面，人们的共同经历少、社群纽带脆弱，另方面，老一代的准精英身份政治不仅具有天然的排他性，且与旧系统血肉相连，我们中很多人最初接触的是这样的“前辈模版”，一些年轻代战友表现出难以区分价

值水平和工具性、标签式的悲观、急功近利等等，都是旧模式的遗毒正在侵染我们社群的警示。切勿指责。要理解到这并不完全是坏事，它更清楚地指出了我们需要修正的底层漏洞。

[image]
[image]

安全文化和广阔的生活

[image] 关键词	安全文化
[image] 关联	[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌
[image] 创建时间	2025年1月2日
[image] **Description**	纸条

当下的生活实在是太狭隘了。

我们被迫困在那些维系现有社会秩序的人设角色和关系结构之中，生命被聚焦于琐碎之事，

聚焦于那些可以被衡量、被明码标价、被买卖交易的东西上。

这种小业主式的贫瘠生存状态如今被强加到了每一个角落。

而真正的生活 —— 那种无限延展扩张的、除了自身能力之外不受任何限制的生活，而不仅仅是生存 —— 唯有在反抗这个社会的斗争中才得得以存在。

因此，我们这些渴望生命扩张、渴望活得尽兴的人们，不得不采取行动，去反击那些强迫我们卑微度日的制度。

[image]

当我们挺身而出，想要夺回生活并使其成为奇迹的源泉时，不可避免地会遭遇镇压。

日常生活中，隐藏的镇压机制每时每刻都在运转，以防范任何形式的反抗，

确保那种维持社会秩序的顺从。

生存的压力、时刻被窥视的潜在感知、路牌上或警察身上散发出的重重禁令、以及我们所处的社会环境结构本身，所有这一切都足以让大多数人循规蹈矩畏畏缩缩 —— 他们低头垂目，大脑空空，只剩下对柴米油盐的焦虑。

但当一个人厌倦了这种贫瘠的生存、意识到生命不该止步于此、不愿再忍受宝贵人生被一天天剥夺时，镇压就不再那么含蓄了。反抗的火星必须被扑灭干净，因为维稳重如泰山。

[image]

生命的延展不可能在躲藏中实现

—— 躲藏不是抵抗，躲藏只等同在社会监狱里换个号子。

但正因为这种延展，这种对自由的张力，促使我们去攻击社会秩序，去采取超越甚至直接违反成文法规或潜规则的行动，

我们始终被迫面临这个问题：如何躲避统治阶级的制服走狗。

因此，我们无法回避安全问题。

我曾经一直认为安全问题很简单，本来是任何人都具备的实践智慧。通过建立志同道合的关系，你可以决定与谁共事；对于不参与行动的人，就无需多言。这是常识，对任何决定反抗支配压迫的人来说都是不言自喻的。

然而，这种实践智慧不能将自己包裹在怀疑和隐秘的氛围中 —— 在

这种氛围下，每一句话、每一个念头都要被审视，甚至连反抗的言语都被视为巨大的风险。

如果我们的实践走到了这一步，那我们就 已经输了 。

[image]

在非法活动的背景下，安全至关重要。

但即便如此，它也不是首要任务。

我们的首要任务永远是创造我们渴望的生活和关系，去开启那种被支配与剥削系统所禁绝的生命的全貌。我们这些真心渴望延展生命的人，希望在所有的行动中都能体现这一点。

从这个角度上，所谓发展“安全文化”的号召，在我看来十分古怪。

当我第一次听到这个词时，脑海中闪过的念头是：“各种保密、各种谨小慎微、彼此疏离……这不正是我们现在生活在其中的专制文化吗！” 街头巷尾和商店里的警察与摄像头，日益增多的身份证件及强制使用这些证件的交互，还有为了“国家安全”而设立的各种武器系统等等等等 —— 这种“安全文化”一直包围着我们，它本质上就是镇压的文化。毫无疑问，作为激进派革命者，这绝不是我们想要的。

“安全文化”倡导者提出的许多实际建议，对于反抗支配制度的人来说，确实是基本常识。显然，你不该留下证据让警察顺藤摸瓜、不该向警察开口，应当采取必要的预防措施来避免被捕 —— 毕竟被捕绝不会永远不会有助于追求自由充实生活的斗争。

但是，把这称为一种“文化”究竟有没有意义呢？

为了避免被捕而必须采取的谨慎，并不能反映出我们想要构建的那种生活和关系。至少我希望不是。

[image]

当无政府主义者开始将安全视为首要任务 —— 视为一种必须发展的“文化”时，偏执就开始主宰我们彼此的关系了。

我们的聚会被设定了层层官僚程序和（实话说吧）监控手段，所有这一切跟我们试图摧毁的体制如出一辙！

怀疑取代了同志情谊和团结。如果某人的长相或打扮不对劲、或者人脉资源不够数，就会发现自己被排挤、被排除在重要的参与之外。

在这个过程中，一些至关重要的东西遗失了—— 那就是我们斗争的初衷。它消失在战斗性的坚硬盔甲之后，我们最终变成了敌人的镜像。

[image]

如果无政府主义斗争不再是去创造一种不同的、喜悦的、激昂的生活，而仅仅是被当成一个需要自我牺牲的事业，那么斗争就会陷入这种毫无乐趣、偏执且僵化的状态。

斗争变得道德化了，不再关乎欲望，而是关乎对错好坏，并被视为绝对且可知的。

这正是激进派圈子里常见的僵化、偏执、以及毫无根据的优越感的根源。

我们成了被邪恶势力包围的“正义战士”，必须严防死守任何被污染的可能。

于是，性格的盔甲变得坚硬，破坏了那种为摧毁支配性世界提供勇气的喜悦精神。

对包围我们的社会监狱的拆除，将带我们直面未知。如果我们带着恐惧和怀疑去面对它，将只会亲手盖起新的监狱。有些人已经在他们的思想和项目中这样做了。

这就是为什么我们的进击计划必须源于喜悦和宽阔的慷慨精神。偏执与恐惧的逻辑、那种一言一行都要斤斤计较的怀疑逻辑，本质上是顺从的逻辑 —— 即便不是顺从于当下的支配性秩序，也是顺从于一种削减生命的道德，它保证了我们没有勇气去面对未知，没有勇气面对那个如果现存秩序被摧毁后我们将置身其中的世界。

相反，我们不如拥抱那充满激情、反抗一切统治压迫的欲望理性。这种理性无比严肃地渴望摧毁一切贬低生命、将生命局限于可量化范畴的事物。正因为它如此严肃，所以它放声大笑。

[image]
[image]

本质主义和身份政治问题

[image]	关键词	不平等 本质主义 社会控制 身份政治
[image]	关联	；
[image]	创建时间	2025年1月3日
[image]	**Description**	纸条

1、

本质主义认为，特定人群存在某种可辨识且客观的核心特质，这种特质是“与生俱来、永恒不变且不可修改的”；群体可依据这些“本质特质”被分类，而这些特质又基于性别、种族、族裔、国籍、性取向和阶级等充满争议的标准。

这些外部特征几乎总是伴随着视觉标记，使得分类更显而易见且/或更易察觉。

这些特征对标记者与被标记者来说均具有社会意义 —— 更重要的是，从反权威视角看，它们蕴含着等级意义：性别特征引发性别歧视，肤色差异滋生种族主义，而任何外貌/行为异于常者都将招致当局的非正常关注。

种族主义、性别歧视、阶级歧视、以及历史上绝大多数压迫形式，都是本质主义所维系并辩护的意识形态与政策体系。

2、

对于遭受种族主义、性别歧视等压迫的个人或群体而言，本质主义可能成为一种强大的防御性视角与反叙事。

身份政治的反本质主义话语并非强化贬损和从属的分类体系，而是试图将历史压迫的范畴转化为颂扬的范畴。

这种转变往往始于对侮辱性词汇的挪用，将其转化为可接受的甚至值得自豪的标签。

曾经意图伤害他者的词汇，由此成为了彰显群体自我的骄傲象征。

“他者”还在那里，只是换位了，使压迫者群体的可识别成员沦为敌人。

无论属于压迫者还是被压迫者群体，都无关紧要 —— 本质主义并非压迫者的专属领域。

3、

反本质主义话语包含无辜论与受害论意识形态，这些理论能迅速将基于共同受压迫历史形成的身份认同，转化成一种优越姿态。

反本质主义似乎证明了受害者永远无辜，因此受害者的行为与反应永远无可指责；所有虔诚的基督徒都深知苦难能使人升华。

压迫绝不是受害者对压迫者做了什么而导致的，因此，受害者选择的任何抵抗策略都是合法的。自卫本身就是正当理由。

4、

身份政治的拥趸们极少（甚至从未）质疑导致受害者身份的标准。他们无法想象，将任何特定的文化建构标记提升到具有重要价值的范畴，竟可能导致压迫。

与压迫者本质主义不同，反本质主义者忽视了权力关系的复杂（这些关系具有条件性和偶然性）；但与压迫者本质主义相似的是，他们都沉溺于自以为是中，坚信自身身份是静态的、独立的、永恒的。

本质主义者通过权力制度化来创造并维系特权；反本质主义者则通过无辜感制度化来实现同样目的。

5、

弗朗兹·法农、埃内斯托·切·格瓦拉、帕特里斯·卢蒙巴，以及许多在无政府主义者眼中声誉极低的第三世界左派（如卡斯特罗、铁托和毛泽东），都激励了帝国宗主国中自诩革命者的一代又一代人，去对抗歧视、种族主义、殖民主义和压迫。这些第三世界民族主义者均在国家主义—— 通常是马克思列宁主义（即斯大林主义）—— 的框架下思考、写作与行动，这一点同样毋庸置疑。尽管如此，作为成功的反帝国主义者这一点点程度上，他们在无政府主义者中仍保有某种吸引力与公信力。毕竟，哪有无政府主义者不反帝的？

6、

自决的哲学和愿景需要诉诸世界政治舆论；这就好像是所谓的革命民族主义者在宣告："我们已足够成熟了，能够自主治理国家、缔结条约、与世界现有国家开展贸易，并控制住社会上那些棘手的异见者。"在某种层面上，这些即将成为民族领袖的人物接受并宣扬了殖民主义的正当性 —— 即土著居民过于幼稚或缺乏教育，无法妥善决定如何开发本国土地的自然资源。

他们试图证明 —— 无论是通过道德力量（如甘地被神话化的案例），还是武力手段（如切·格瓦拉等人被浪漫化的案例）—— 自己值得被认真对待、进行谈判，并最终在治国之道上获得平等的伙伴地位。

殖民强权划定的国界将被奉为圭臬，贸易协定通常（或终将）与前宗主国缔结，殖民统治者制定的镇压内部异议的法律将继续沿用 ……本土资产阶级接管了所有政府机构，通过诉诸明确的跨阶级民族团结理念，将剥削者与被剥削者之间最根本的斗争转移了视线。

7、

1960年代末至1970年代初，欧美兴起的基于性别与种族的解放运动，其思想理念与行动正当性均源自这些成功的反殖民斗争。第三世界民族解放的修辞被反复援引，以至于许多非裔美国人、部分女性及其他自认受压迫群体开始将自身定义为"内部殖民地"。

等级社会的精英已经将各种少数群体定性为从属的“他者”；将殖民剥削者及其机构简单地视为压迫性的“他者”，正是身份政治问题的核心所在。

将责任和罪责全盘归咎于被归类为压迫性他者的群体， 扼杀了超越等级与支配的可能性 ；这种操作仅仅 颠倒了 特定阶级或群体被赋予的价值，却无视个体在历史或当代压迫中的 共谋关系 。

8、

对大多数女性解放主义者而言，"女性"这一类别 —— 被简化为仅基于性别的封闭范畴 —— 成为唯一重要的分类标准。女性遭受的贬抑与压迫无处不在：歧视、强奸及其他形式的暴力、骚扰、对母职与异性恋的期待和强制，以及无数维系女性依赖与顺从的手段。女性解放主义者将父权制宣称为敌人，其中部分人更进一步，将男性 —— 这个仅基于性别而被简化为封闭类别的存在 —— 视为敌人。

对大多数黑人民族主义者而言，"黑人"这一类别 —— 被简化为基于遗传学和种族的封闭范畴—— 成为唯一重要的分类标准。黑人遭受的贬损与压迫无处不在：吉姆·克劳法式的歧视、私刑及其他暴力形式、骚扰（尤其来自执法部门）、对奴性态度的期待和强制，以及无数使黑人保持依赖与顺从的手段。黑人民族主义者将白人种族主义宣称为敌人，其中部分人更进一步，将白人—— 这个同样被简化为基于遗传与种族的封闭类别 —— 视为敌人。

9、

种族和性别，和其他具有文化特异性的意识形态建构一样，既真实又虚幻。在生物学意义上虚幻 —— 对这些区别的理解与非文化性的客观范畴并不对应；在社会学意义上真实 —— 无论特定的文化背景如何，都有清晰的方法来辨别种族主义、性别歧视和其他形式的统治和剥削。因此它们值得批判性关注。

性别研究的倡导者在分析和打破对性别理解的偶然性方面做得非常出色，表明特定的染色体和生殖器组合仅仅是构成性别意义的一部分（而且可以说，甚至并不是最重要的部分）。批判性种族理论也是一个令人鼓舞和有趣的反本质主义的最新发展。

10、

殖民主义者及其辩护者始终在鼓吹统治的神话意识形态范式。反对等级制度的人早已洞悉并预料到这一点。而反帝国主义者（那些理应反对殖民行为的人）在观念上的主要矛盾，在于他们自身也接受了老帝国式的偏见与刻板印象 —— 只不过价值观颠倒了一下。

那些为种族至上主义者和性别歧视者谋取私利而创造并维系的贬损性“他者”范畴（黑人、野蛮人、女性）从未被质疑；其客观性不言自明，根植于种族主义者与性别主义者最初塑造的文化常识。

人人都能分辨男女——这是生物学事实。人人都能分辨黑与白——这

是科学。早在欧洲殖民主义形成之前（尤其在其形成期间），科学和生物学就被视为辨识“客观现实”的方法。

11、

群体自我定义似乎契合无政府主义的自我组织与自愿结社原则。反本质主义的身份认同甚至可被理解为试图重构基于血缘的共同体 —— 这种共同体已被工业资本主义的强加所摧毁（该制度基于劳动分工，导致个体彼此间的疏离/原子化和异化）。

然而这种身份认同仍存在问题，因为它是在受害者意识形态框架内锻造的产物；其根基恰恰是那些曾被用来合理化压迫的任意构建的分类体系。

⛔

建立在视觉标识基础上的所谓解放性反叙事，永远无法真正质疑压迫性意识形态的正当性。另一个问题在于对意识形态构建的身份认同的推崇 —— 它要求群体忠诚和团结凌驾于个体真实生活经验之上。

12、

任何团体（无论是受压迫群体、等级组织，还是任何倡导统一的团体）所承诺的归属感，必然要求被吸引者接受他人预先设定的区分与分类体系。一旦反本质主义者接受了包容/排斥的边界（这是通往分离主义的第一步），他就无法以其他方式定义自己或被定义了；反本质主义叙事中既有的标准成为了唯一有效的准则。

这种身份原教旨主义要求任何追求根本性变革的人放弃自我定义的能力。

必须将自我意识完全溶解于既有的意义范畴中。生物学 —— 无论其背负多少意识形态和文化枷锁 —— 即是宿命；主体性只能被牺牲或

压制。威权主义的首要谎言便是：所有他人都比你自己更懂你自己。

本质主义者只需对选定的他者略加瞥视，便自认洞悉其全部本质。分离主义者、民族主义者、反帝国主义者—— 都是本质主义者 —— 竟将此称之为“解放”。

[image]
[image]

街头政治对抗技巧提示（就是打架）

[image] 关键词	搏击 自卫 街头 防身
[image] 关联	
[image] 创建时间	2025年1月4日
[image] Description	纸条

[image]

最近几年有些习武热出现。我也观察过一些，重点关注直接以防身（而不是健身）为名的培训项目。但总体上可以说，大多是没在街上真正打过架的人在那教学 - 换言，这些所谓的防身训练，很可能并不具有太多实战能力，尽管艺术性不低，挺出片儿的。

目前在国内练格斗的中国人似乎没啥街头政治对抗的经验。留过洋的人应该有一些至少是旁观角度的经验，尤其是本世纪以来法西斯猖獗，政治性街头搏击基本已经自成一体，尽管专门的培训项目不太常见。

不论如何，有一些小经验，每个有可能面对风险状况的人都值得关注。

简单总结如下：

1、作为商业项目最常见的所谓综合格斗训练，其实在街头对抗的背景下意义不大。

至少没必要专注于擒抱训练。即便练好了也只能应聘个保镖啥的，而且还要祈祷别遇到啥大状况。所有地面技都如此，什么巴西柔术摔跤啥的，都基本是赚钱的生意，不是傍身的本事。

站稳才是防卫的根本。如果你跟一群人打架，你跟其中一个对手一起倒地的话，立刻就会有人踢你的脑袋或者背后捅你一刀，一切会在一秒钟内发生。如果你想活下去，那就要让自己在任何情况下都不要倒地。

2、避免那些具有千年高贵传统的花哨技术，不管是日本的还是中国，除非你只是为了传承艺术跟大佬合个影啥的。这些东西都是为封建时代的职业种姓发展起来的，需要多年的全日制学习才能掌握并且基本涉及不切实际的过时的武器。除非你是地主士绅有能力做个武士。否则，关刀武士刀这类东西跟火车模型收藏没啥区别，都是玩物。想在街上活下来，玩物派不上用场。

3、如果你从来没接触过武术，感觉自己没有天赋，但很想要在遇到流氓时能自卫，那就练习一些最基本的东西。比如踢腿，拳打脚踢，在徒手搏击的情况下必须的技能，泰拳对此有好处。如果你预计会遭遇到持有武器的对手，不管是钝器还是锋利武器，菲律宾武术会有帮助，比如Kali或Escrima。如果你住在一个遍地是流氓并且每个流氓都有枪的地方，那你就只能给自己弄个好枪，去练打靶。

4、不必专注于装备，包括武器。如果你会打，身边的一切都可以是武器，相反，如果你不会打，手持关公大刀也很可能挨揍。

即便你只准备徒手搏击，也要首先考虑指关节安全。你不能戴着搏击手套到处走对吧。但如果你第一拳都把手指打断了，那就没有然后了。所以手部的安全是要点。

5、不必花太多时间研究缴械技术。 实战中最可能的情况是，你根本没机会用上缴械技术。缴械尝试总是极其危险的。除非你的对手明显喝醉了，或者完全没有经验，并且周围还没有其他对手的情况下，你才应该尝试缴械。否则，你不应该试图解除对方的武装，相反，你应该尽可能使用你自己的武器。如果你没有自己的武器，又没有办法逃脱……那就真的有麻烦了。

6、自卫大师经常说：“首先，你应该尝试逃跑”。通常情况下的确如此，但并非总是如此。首先，抓住对方总是比逃跑更容易，所以，除非你相信自己肯定能跑得比对手更快、并且准确地知道逃生路线的情况下，逃跑才有意义。其次，你可能不是唯一一个生命和健康受到威胁的人，如果你能逃脱，但意味着抛下同伴，你还会跑吗？

显然，保持良好的体形并进行有氧训练总是有利的。几乎所有的街头对抗都需要耐力和至少一点短跑的技能。但你始终应该为无法逃跑的情况做好充分的准备。

7、跟专业人士一起训练是有必要的。尽管的确很多这方面的专业人士都在捞钱、俱乐部乌烟瘴气、培训师麻木不仁，都挺普遍的，但还是要有专业教练才行。只是不要被动听从教练安排所有东西，他跟你的优先事项很可能不一致，你要以自己的战略为指导，为了自己的需求，去请教专业人士。

你的目的是为了应对严肃的对抗，那就需要请求至少一个陪练人员，一个或者多个，多人的场景更真实。如果你的教练不了解陪练的重要性，那就换个教练。

[image]
[image]

解放教育101:如何培育潜在的同道

[image] 关键词	团队 教育 解放 革命
[image] 关联	
[image] 创建时间	2025年1月5日
[image] **Description**	纸条

保守气氛越来越浓？志同道合的朋友太少？怕吵架不敢谈政治？... 别急，同道是可以培育的。

对解放者来说，培育同道的过程绝不是指导说教，那是违背我们原则的。我们追求的不只有革命、更非仅限于政权更迭或政策改革，我们的目标是终结支配和压迫，消除等级和奴役，这项工作无法在街头一次性实现，而是首先需要在更多人的意识和内心中实现 —— 换句话说，这需要从教育开始，从人际结构的革命实践开始。这项工作是未来的街头后是否能避免重蹈覆辙的重要基础。

[image] [image]

如何推动变革者的志趣朝向解放性政治的方向进展，是构建真实的解放政治力量的过程中至关重要的环节，这一环节充满挑战，但极具价值。诚然，整个过程格外耗费心力、难以驾驭，且往往冲突不断。

本文希望提供一些工具、策略和框架，帮助大家以既能保持持续进程的开放性、又能保护参与此项工作的同志们的边界和精力的方式开展这项工作。

首先，请审视您自己在培养同道的过程中的自我定位。您是否带着某

种先行者的优越感，将他人视为可灌注“进步”知识的容器？若然，即便可成，也注定徒增艰辛。

👫

解放性的教育其本质应该是共同成长的过程，核心在于与人建立解放性的关系：既要挑战对方的固有认识，也要允许对方反过来挑战您。当有人自诩比当事人更了解其生活、还准备好现成的“答案和/解决方案”时，人们理所当然会抵制这种“说教”。

准备好参与解放进程的我们，必须致力于培育同道 —— 向同道学习，与同道共同成长。切勿因自以为知晓对他人来说的“最佳”选择，而将人禁锢于旧式的教派思维中。

即便在罕见情况下的有人将您的言论奉为真理或福音，也请记得这根本不是表面看起来的“积极”结果。多数人从小就被训练着去复述他人的政治分析却缺乏独立思考，哪怕复述的是革命理论，也绝非解放的模样。

开展解放性教育时，我们追求的理应是帮助人们建立新的思维方式，构建自主分析能力，而非简单模仿我们的观点和主张。我们需要协助人们建立政治自主性，摆脱对他人意志的绝对屈从。

[image]

需要在不同阶段为人们保留充满同理心的空间，同时明确传达成长的期望。这里有一个很微妙的平衡。若未能把握恰当平衡，结果要么彻底疏远对方，要么完全无法激发其改变的动力。

培育同道的过程需要在不同阶段为人们保留充满同理心的空间，同时明确传达成长的期望。若未能把握恰当平衡，结果要么彻底疏远对方，要么完全无法激发其改变的动力。

关键在于，您应该认识到：为他人保留成长空间，绝不等同于放任有害行为或信念不受质疑。若缺乏问责，人们便无法学会更善待他人。

在此过程中，既要保持同理心，更需坚守边界。

我们不仅在传授全新的经济理论，更重要的是一起探索超越支配与控制的全新的人际关系模式。

除非我们亲自来践行兼具慈悲与边界的相处之道，否则无法实现这种转变。

“我理解你形成这种信念的缘由，但此论点存在缺陷/具有危害性”—— 这样的沟通方式效果显著。

👬

多数人渴望被理解、被“看到”其立场的成因，当您主动“看到”对方的内心并展现出这种尊重时，他们便更容易敞开心扉接纳新观念。

一定要留面子。

给人们留有保全颜面的余地。

多数人会将自我尊严与立场相捆绑。传达完您的观点后，要懂得适时收手，让对话自然转向而不致令对方承认“失败”。

往往只需播下种子便已足够 —— 这并非意味着对话终结，而是人们需要喘息空间。他们需要时间静坐沉淀，咀嚼新观念与新概念。日后再去追踪这些种子，并悉心照料，机会自会出现。

人们常会主动重提旧事，有时甚至表现得就像是自己从未反对过一样。若条件允许，不妨顺其自然 —— 请记得，此刻能推进对话才是关键。其余都不重要。

强调“顺其自然”，是因为我们往往低估了让对方保全颜面的价值。虽然有时必须采取强硬手段，但多数情况下，将胜利内化为个人成长，而非炫耀于人，才是更明智的选择。

每个人都有自己的切入点。统治系统总会以某种方式压垮每个人。倡导，就是找到那个切入点，借力揭示对方真正的利益所在。

深入了解对方，建立关系纽带，您自会发现他们的切入点。比如，他们的上司很糟糕吗？当他们抱怨时，既要表示同情，也要点明其糟糕的根源。没错，上司人品低劣，但这种低劣正源于他们能从替自己劳作的人身上牟利 ——这是等级制度特权造成的 。我们若能联合起来创造没有等级制的合作，岂不是能做得更好？…… 这就实现了提示。

[image]

注意：尽可能避免使用敏感术语：比如无政府主义、共产主义、自由主义、资本主义等等概念虽重要且值得普及，但是在培养同道的初始阶段，这些词语的使用几乎必然会适得其反。请记得这些词汇对多数人来说都很容易引发联想 —— 他们一生都受制于庞大的宣传机器（就算厌恶新闻联播，也并不意味着就能理解问题所在和错误根源）。这些政治词汇自有其适用场合，但绝非初次接触时的“寒暄”。请尝试用不提及“无政府主义”一词的方式阐述其理念和价值。

如果感到困难，建议多阅读相关入门书籍，能帮助您找到更简明的表达方式。可以在物料站点《炫》的书籍专题中寻找对您有帮助的书籍。

切勿低估研读大量理论/政治书籍及播客的价值 —— 即使您已经掌握基础知识，聆听他人向新朋友阐释的语言表达，都可以助您提升自身的阐释能力。

和大家一起阅读也许效率更高。一起探讨，促进头脑风暴。

[image]

最后，请区分愿意成长的人与彻底拒绝改变的人。对于后者，您可以为改变留有余地，但切勿陷入无谓的循环辩论。守护您的能量。所谓“建立有同理心的边界”，关键在于认识到您只能与愿意且有兴趣参与对话的人进行这种工作。您无法强迫他人改变，只能提供支持。对于执意持续伤害他人者，慈悲的边界或许意味着割裂关系。

在此过程中也请善待自己。你我都并非完美，一直都在学习成长。若对话中遇到无法解答的问题，不必苛责 —— 将其视为需要深耕的课题。

归根结底，培养同道并无固定步骤，因为每个人都是独特的个体。也正因此，本文强调过程而非提供具体的操作指南。解放性教育终究是关系的构建。请放慢脚步，发展自己的分析能力，学会设定并维系充满同理心的边界与关系规范，以促成改变。保持耐心 —— 有人进展缓慢，也有人领悟迅速，但无论如何，参与其中都是非凡而充实的生命历程。

[image] [image] [image]

[image]
[image]

精英主义语言的问题 - 与激进派中产阶级活动家一起探讨

[image] 关键词	会议 协调 团体 战术 教育 沟通 研讨会 组织
[image] 关联	
[image] 创建时间	2025年1月6日
[image] **Description**	纸条

接受体制教育后仍能保持独立思考的积极和反叛创新的能力，是非常难得的。尽管中产阶级激进派人士不多，但他们的存在意义重大。然而，跨阶级的沟通、尤其是辩论和倡议活动，经常出现因理解障碍而导致的冲突。

对此，我们也许可以提出一些建议 ……

本站主题“安全性”包含前线社区自行主持的培训/教育工作。对此，公信力是比技术水平更重要的前提。公信力也是团结能力和亲和力的重要基础，但很容易受损。

下载打印版：

https://drive.google.com/file/d/1uSCtPpW3PR34xvLq-bQ-50kViqTXIjZA/view?usp=sharing

精英主义语言的问题常出现在中产阶级、受过高等教育的人试图与所谓的“普通大众”沟通的情况下。如果沟通的目的只是商业活动，那只需把语言简化至目标受众群的中位水平即可，或许再借鉴一些目标群

体的流行语和文化符号，就能确保销售成功。

不过，若动机更具公益性 —— 例如中产阶级活动家试图与其他背景的活动家沟通，或者在向“普通大众”分享信息、资源和观点时，问题就变得复杂多了。

出于充分的历史原因，学术界惯用的语言（即许多中产阶级活动家驾轻就熟的表达方式）往往会令受教育程度较低的人感到疏离或困惑。然，从父权制到帝国主义，这个世界面临的种种问题皆为系统性病态，需要严肃的努力与专注才能理解。而与我们理解这些问题形成直接对立的，是前所未有的强大文化机器。它操纵着每个人的价值观、意识形态、历史乃至语言本身，以维护既得利益格局。

我们如何使用已被文化产业严密控制的简单语言，向注意力持续时间日益缩短的普通大众，以简短易消化的片段，来阐释复杂晦涩的理念？

显然答案是不能。我们必须认识到：语言在当代社会已被用作控制工具，而词汇量缩减、语法简化、注意力持续时间缩短的趋势，正是人类历史上最有效的去能力化手段之一。

抵制语言的愚民化，培养批判性思维能力，其重要性不亚于争取社区自治和经济自足。

语言必须成为革命的阵地，它是所有社会斗争的必要武器。

作为中产阶级活动家，我们的责任是用我们所受的教育帮助复杂的专业语言变得易于理解，而不是将大多数人无法立即轻松理解的事物视为本质上难以理解的。

但若暂且搁置对理论长远发展的探讨，回归当下语境，那些关于语言晦涩难懂的批评确实具有相当的合理性。这些批评在其他场合均有阐述，其核心在于承认：体制教育是少数人（尤其是国家层面的“核心身份集团”）享有的特权；当我们使用伴随体制教育而来的精妙语言时，会阻碍未受过此等教育者的理解和共情，并有意或无意地将激进

组织与运动中的话语权牢牢掌握在受过体制教育的精英阶层手中。当这种批评被教条化时，通常（错误地）简化为：长词与复杂句式即为特权象征，而特权本身即为恶。这种教条化批判忽略了关键认识：当前的教育是特权没错，但这正是需要拆除的部分—— 将接受高等教育的荣耀普及化，让人人都能享有。

如果这些批评的根本目标是挑战语言中的精英主义，那么激进主义文献中就会出现精妙程度高低参差的语言的自觉结合，让每个识字者都能接触到既在其舒适理解范围之内又超越其舒适理解范围的材料，既欢迎他们又挑战他们。

特权活动家本应自觉运用语言以促进理解，而现实中却呈现两种极端：受过教育的激进分子要么漠视问题，无视潜在受众中教育程度较低的群体；要么就是条件反射式地回避专业词汇、回避复杂分析和深入（即冗长）论述，以逃避问题。教育被斥为资产阶级产物，或用当下更时髦的说法——“排他性”象征。活动家们非但没有解决问题，反而与主流喉舌及体制教育沆瀣一气，共同参与了针对本应作为赋权对象的群体的智力屠杀。

要对精英主义语言进行战术性考量，就应当审视批判此类语言时所蕴含的若干预设。其中最根本的莫过于“大众”的神话。其逻辑如下：”大众缺乏教育，使用艰深词汇会疏远他们”。但究竟该如何划分精英与非精英的界限？“大多数人”会使用“精英主义”这个词吗？（天哪：精英主义这个词本身难道不就很精英主义吗？）写作呢？诚然多数人都是识字的，但许多人因非自身过错而文盲。文字记录是否精英主义？活动家难道不该制作传单和宣传册？这显然排除了不识字的人群……受过教育的活动家正以居高临下的姿态设定可接受的”愚昧”标准；即便他们排斥学术语言，却通过维持智力的等级制度来捍卫了精英道德，只愿站在阶梯上降到特定位置来迎合教育程度较低者。任何仍被排除在外的人，都只是被他们对“普通人”概念的构想所遗弃。

“大众”神话的影响在于，当我们走出自己的圈子时，多数活动家会对那些他们认为没有大学学历的人居高临下地说话。实际上最明显的信号就是听众是否贫困或是否少数族裔。我认为许多活动家甚至没有意识到自己通常有多么的傲慢，当他们试图使用明显不属于自己的语言时，这种傲慢是多么地显而易见。然后他们转身又谈论精英主义？……

禁止所谓精英主义语言的禁令，还暗含着对贫困背景人群的刻板印象—— 认为他们要么无法获得优质教育，要么根本不愿学习。事实上，在许多贫困社区，接受良好教育都被视为一种赋权方式，但鲜有活动家在与弱势群体交流时试图淡化这种教育背景。特权活动家通过在圈外回避学术语言和分析，维持着一种依赖关系——他们充当知识守门人，永远需要他们来将法律条文、科学研究、政治分析等转化为“通俗语言”。

批评中另一个隐含的假设是，某些语言类型天生具有精英主义倾向。这是错误的假设。事实上更丰富的词汇量和更复杂的语法结构是极有价值的工具，尽管人们需要接受更高教育才能驾驭这些东西。真正具有精英主义色彩的并非语言本身，而是这个国家资本主义、种族主义的教育体系。受过体制教育的活动家们肩负的使命，正是让这种教育普及化，并将语言转化为大众可用的工具。我们不想要为大众量身定制的奥威尔式新话，我们要的是解放语言本身 - 语言的去神秘化。

遗憾的是，受过教育的活动家们仍在浪漫化所谓的“平实语言”，同时继续抱怨大众如何再次被政客们最肤浅粗糙甚至陈词滥调的诡辩所蒙蔽——这些话语经媒体传播后，竟又一次煽动了对最新的战争或严苛政策转向的支持。将各种语言形式从当前特权等级中剥离出来，置于多元平等文化的应有之境，是至关重要的行动（前提是先让社会中不同文化水平的人们享有平等的地位）。

事实上，许多针对精英主义语言的现有批评本身就带有精英主义的色彩，因为它们旨在维系制度化教育者对分析性话语的垄断（这些教育者本身往往已被制度化，而非激进派，就算其以异议自居，也很可能并非站在我们这一边）。受过教育的激进分子对任何带有精妙色彩的语言的排斥，反而使激进分子自身变得愚昧。未受高等教育的激进分子也并非更具无产阶级属性或包容性，他们只是更缺乏成效。

颠覆教育体制，再用解放性的教育来推动颠覆，岂不是更有效？我们应当揭露并打破父权制规范 —— 那种认为你的一切都应该被“管起来”、高高在上压制所有质疑和反驳的规范。我们应当运用自如的语言形式—— 无论学术的还是日常的 ——只要表达清晰，能激发知识的传播与共享。这将使周遭受益。同样，学习他人使用的语言类型亦能启迪我们。承认语言的多样性，但要打破这些语言所处的经济、种

族和性别等级制度。

[image]
[image]

如何选战友

[image] 关键词	亲密团队 关系 团队 战友
[image] 关联	[image]您需要真正的自己人-如何组成一个亲密团队：街头实战指南S05E09
[image] 创建时间	2025年1月7日
[image] **Description**	纸条

有朋友问“如何选战友”。我认为至少有两点是需要考虑的：历程，和心术。

历程即心路历程：关于一个人是如何得出TA认为值得秉持的政治立场和见解的。

- 有些人通过读书，他们很幸运地从一开始就没选错读物。
- 有些人通过交往，受到周围人的熏陶，被归属感吸引。
- 还有些人比较前卫，追求叛逆时尚。

其实这三种情况都很难得到稳妥的战友。

准确说是，仅仅这三种是不够的。

第一种人可能不擅长思考，容易被更狡猾的宣传所蒙骗，被宏大的音量所吸引，在心理战中垮塌。我绝不是说读书不好，读书至关重要，

每个人都应该尽可能多读书；但是，被书说服、还是借书提升，则是截然不同的两件事。

第二种人就更糟了，他们很大程度上只是擅长混圈子，简称搞人，而不是搞志业，其战略目标从一开始就错了。作为情绪价值黑洞他们可以被几乎任何能供应情绪价值的人际关系“网”住 —— 今天是你，明天就可能是你的意识形态对手。也相比下也更容易成为告密者（甚至可能都不知道自己在泄漏同伴的致命信息）。

第三种则有点遗憾。他们骨子里有着珍贵的反叛精神，可能很容易被朋克嬉皮士亚文化所吸引。但是否真的能在解放斗争中有所建树，则是另一回事。天生的叛逆不会长期支撑革命的创造力 —— 如果您也了解主流体制是如何擅长收编小异议从而消杀掉他们的变革能力的，就无需过多解释。

更可靠的心路历程则来自两方面：首先是作为基础的内观 - 即 对自身的精神洞察力，深入的挖掘和洁癖般的自我诚实。能做到这点的人很难被权力的谎言所蒙骗而做下违背自身尊严福祉的行为。你不需要给TA讲解为什么鱿鱼游戏是卑鄙的迫害性的、为什么采掘主义是没有未来的，等等大道理，每一个作为人类对自己诚实的人都不会在大是大非上误判。
其次就是实战，没有任何书斋能比得上从实战中获得的学习 - 那是一种灵性，寻常文字不配用来描述它的美和深刻。

如果你身边有从这条路走来的朋友，千万拉住，别放手。

至于心术，可能更多人熟悉其灾难性所在 - 同等的苦难经历催生出截然不同的善恶两级。有的人相信以暴制暴、以战止战、以狠抗狠的有效性，他们被残害得更为深刻；他们可能亲手杀死敌人，却同时亲手将自己变成了敌人**2.0**。就像俗话说的“多年的媳妇熬成婆”，白瞎了半生的煎熬，最终却传承了婆媳等级的剥削压迫。

能从苦难中得到滋养的方法只有一种，那就是，识别苦难的根源，并铲除它。

一个好的战友自带这两方面优势。如果没遇到也别急，一定程度上它是可以培养的。

[image]
[image]

需要解决方案，而不是恐惧

[image] 关键词	大规模监视 安全虚无主义 社会控制 资本主义 高科技镇压
[image] 关联	[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人
[image] 创建时间	2025年1月8日
[image] **Description**	纸条

格雷伯曾经把资本主义下的社会控制体系描述为“一个庞大的官僚机构，专门用于制造和维持绝望，一种巨型机器，其首要设计目的就是摧毁任何关于可能的替代未来的感知”。

这台机器的操作者得到了绝望者自身的协助，原因很简单。几乎每个人都害怕自己的结论被证明错了，尤其是对关键结论而言 —— “希望”这个东西是否存在，就是这样的关键结论，犹如一个挂在悬崖边紧抓着唯一一根绳子的人对于“应不应该松手”的判断。一旦被证错误其后果摧枯拉朽。

如果“希望”最终被证明确实存在，而一个人早已永远滴放弃了它 ……那会怎样？

如果你放弃了自己最珍视的梦想，多年后却发现它一直就在你触手可及之处，只要你花一点点勇气去追求一下就能得到，你会感到多么痛苦？

为了避免这种命运，无数业余的末日预言家不遗余力地试图说服人们：「所有革命注定会失败，不如现在就直接放弃」。他们的精神导师是梭罗，他在其著名著作《论公民不服从》中，以严谨而精妙的论

述主张废除政府 —— 但却又轻描淡写地否定这一想法，称“那永远不会发生，所以我们只需做些政府不喜欢的小事，祈祷他们不会开枪。”

梭罗的智力后裔们直到今天仍在继续他的追求。其中一些人喜欢指出帝国无以伦比的威力，作为证明“替代未来”永远不可能实现的证据。

更精明的悲观主义者，或许意识到看似不可战胜的军队在历史上曾多次屈服于革命，于是更倾向于关注当今统治阶级使用的心理和宣传武器，并拼命把它描述得无比强大。

在这一派的论述中，你很容易遇到杰里米边沁著名的“全景监狱”概念。这是一种监狱设计，据称只需一名守卫就能控制众多囚犯，因为建筑布局使囚犯无法判断自己是否正在被监视，因此必须假设自己始终处于监视之下。对此，无数檄文只是激起了安全虚无主义，它们试图让人们相信，当前监控摄像头、数据库、智能手机和国安大规模监控项目的泛滥构成了不可逾越的障碍令任何起义都不再可能。

而他们好像完全忘了，原版的“全景监狱”作为监狱设计完全失败。然这一概念却在几个世纪后仍然在以边沁自己可能都从未想象过的方式继续履行其使命 —— 为那些自命不凡的书斋理论家提供修辞弹药，试图说服人们“抵抗是徒劳的”。

斯诺登就著名地撞上了同一个坑，他冒死搞到的东西只是让无数人相信了“无能为力和不可避免”，而不是详细分析如何去击败它。

当然这些人都没读过堤昆。

了解情报理论的人都知道，棱镜那样的东西只是表面上看起来威力无比，事实上它的存在是情报失败的标志。但很遗憾人脑就是如此追求简略，对于任何倒霉事，人们都倾向于宁信其有。如果朋友和敌人都在讲述同一个故事，那它一定是真的，对吧？嗨 那可不一定。

对抗绝望机器的第一步就是不要相信它所说的一切。或者，至少不要帮着重复它…

[image]
[image]

技术与权力

[image] 关键词

[image] 创建时间 2025年1月9日

[image] **Description** 纸条

[image]

[image]

建设中！敬请期待。

[image]
[image]

走出部落

[image] 关键词		关系 沟通 社区
[image] 关联		
[image] 创建时间		2025年1月10日
[image] **Description**		纸条

将一些不怎么“志同道合”的人组织在一起形成一个社区的结果是什么？有可能很有趣，并且很有意义。但为什么很少有人会这样做呢？究竟什么是”事实”真的可以统一吗？

[image]

我们的文化中发生了一些奇怪的事。两个看似矛盾的趋势正在并行发生，似乎还没有多少人注意到。

我们生活在一个追求真实性的时代，痴迷于自己的衷心和诚实；我们告诉孩子保持追求自己梦想的激情，因为大家都认为迫使某人与他们的真实自我发生冲突是一种压迫感。整个社会都在拼命寻求诚意，不论是对周边的彼此还是对政治领导人。我们重视浪漫的爱情，因为它源于自发的、不受约束的感觉。它是真实的，因为它是无中介的。真实性是新的文化货币。

然而，尽管对真实性有这种痴迷，但同时却正在失去对真相的控制。我们生活在后现代的时代，其中旧的元叙事似乎已经变得狭隘和令人难以置信。对公共机构的批评不断增加，而社会信任水平却在不断下降。

阴谋论比比皆是，和其他形式的医学、学校教育和新闻学一样 —— 甚至有时在学术上被称为
“非主流认知”。这涉及所有积累知识的领域。科学和宗教的基础都受到了攻击。怀疑和认知的不确定性困扰着人们提出的每一个问题。所有这些都是我们目前所处的后真相时代的特征。

因此，对真诚和真实性的关注与所有形式的集体权威的腐蚀化共存 —— 无论是宗教的还是科学的。那么怎么才能理解这个问题？

这些趋势实际上是同一枚硬币的两面，而知识社会学至少可以解释为什么。

知识社会学关注的问题是：知识的社会条件是什么？它的前提是我们在很大程度上由于所处的社会环境而导致我们持有某些信念，并研究某些环境如何使我们或多或少地相信某些事。知识社会学并没有对真理本身提出主张。相反，它关注的是我们可能称之为知识的主张。

这里有一个例子：如果你是在一个原教旨主义的基督教社区出生和长大的，从未接触过任何有关宗教或科学真理的竞争性观念，那么知识社会学就会认为你不太可能怀疑你的原教旨主义父母的教义。因为原教旨主义的基督教环境具有强大的合理性结构。

这意味着，如果您在社交环境中遇到的一切 —— 您的家人，朋友，邻居，学校课程，假期等等 —— 都在加强并支持您所信奉的知识框架（在这种情况下是基督教原教旨主义），那么你就没有理由质疑它的合理性。为了简单理解这点可以推荐一部小说《幸存者》。无疑，我们生活的社会环境可以强化或挑战我们持有的信念，使我们或多或少地怀疑它们（这就是为什么基督教原教旨主义者如此担心公立学校教授的内容，也是为什么政治宣传必备的工具是封闭）。

知识社会学并不假设所有对知识的要求都是正确的。仅仅因为有人绝对肯定地认为，进化论是错误的，并不能证明这一点。相反，知识社会学家有兴趣了解允许这样一个人存在的社会过程。换句话说，知识社会学区分了真实存在的真理和人们如何形成对真理的信念。这种区别对于理解当代文化至关重要。

知识社会学本身的社会学 - 在工业革命之后出现，作为一种解决向现代性转变所带来的后果的手段。人类学家和社会学家将前现代社会理论化为特征，其中包括强有力的合理性结构。生活在相对同质的社会中，长途旅行既罕见又困难的人们，不太可能遇到可以从根本上扰乱他们既有观念的人或想法。

正如 Berger 在他的经典著作“无家可归的心灵”和“异端的迫切”中所写道的，传统或前现代人过着命定的生活，在这种生活中，由于社会条件（而不是认知缺陷）人们更难以质疑被认可的日常生活。然而随着技术的发展、流动性的增加和多元化的发展，现代性的转变已经出现。根据 Berger 的说法，现代化进程削弱了合理性结构，因为它使我们每个人都暴露于多种道德、政治和宗教的选择之中。

如果我的邻居崇拜的神与我不同，我更有可能质疑我自己；如果我爱上了一个与我不同政治意识形态的人，这可能会鼓励我重新思考我自己的承诺；如果我看到其他人兴旺发达，他们以与我的信念完全不一致的方式组织自己的生活，我可能会开始怀疑他们知道我所不知道的事。这些都是现代化的结果。

当然，Berger 在20世纪70年代后期写下的这些书，可能无法预见全球化和互联网的发明将如何加剧现代化进程。全球化增加了全球人民和文化产品的流动，而互联网提高了我们对人类生活的广泛多样性的认识，这两者都严重削弱了可信性结构。因此，两者都侵蚀了外部的权威来源，使得确定性更加难以捉摸。

然而，个人需要一定程度的认识自信心才能过上自己的生活。我们不能一直犹豫不决。因此，Berger 认为，随着现代化的进展，个人将自然地寻求认识论权威的新来源。

Berger 认为，在可信性结构薄弱的环境中，个人更可能会确定性地进入。也就是说，他们会将自己的主张归功于个人经验。我可能不确定论文中看到的内容、或者我的牧师告诉我的东西、或在网上看到的视频的可靠性，但是我可以肯定的是我自己的经历。我知道我经历过什么和我的感受，没有人可以拿走这种经验。Berger 因此认为“现代化和主观化是同源过程”。

由于直到最近组织我们社会的意义和真理的共同框架变得严重可疑，个人开始寻求其他地方的认识论权威。反过来，个人经验成为了真理的全部和最终结果。

因此，我们今天如此专注于真实性并不奇怪。如果个人经验是真理的基础，那么一个人必须忠于自我和自己的经历，否则就是谎言。我可能会在实质上不同意你，但只要那确实就是你自己的经历，那么我能说的就很少了。

当然，虽然这种逻辑可能反映了今天的文化常识（考虑到我们的社会条件）但这并不能使其为真。在某些情况下，我们的主观感受可能是行动的有用指南，但它们常常使我们误入歧途。无法保证我的感受和个人经历会与经验现实保持一致。我可能对气候变化的本质有一定的了解，但科学的同行评审研究更有可能确定究竟发生了什么。

另外，仅仅因为一个人是真实的并不意味着他们是对的。在这个世界上有很多人仍然忠于自己，但仍然是愚蠢的和自私的。最后，如果一个人的内心感受是正当的，真诚只是一种美德 —— 如果此人本身是一个混蛋那么心里话说出来也是错的。

所以这就是我们的困境：后现代性的特点是弱合理性的结构，使我们共同的意义和真理—宗教和科学性质—的框架变得越来越容易被怀疑。这鼓励人们进入认识确定性，但这只会增加人与人之间的距离，从而使得没有可以为我们的主观感受提供急需纠正的共享框架。

如何克服这个问题？除非回拨时钟（这看起来非常不可能，而且由于许多原因，也非常不合适），因此其中大部分似乎有些不可避免。因此，当下比以往任何时候都更需要的是一种协调性的、集体的尝试，以复苏那些在晚期现代性中充当反对主观主义的堡垒的机构和传统。

换句话说，虽然可能永远无法达到前现代社会中人们所经历的确定程度（这不一定是坏事），但我们当然可以确保某些知识主张比其他主张更重要。

这主要应该是大学的工作。学术机构需要站在识别和制裁良好知识、

区分善恶与真相和阴谋之间的最前沿。媒体和记者也是如此。方法论的严谨性和共同的评估标准是必须建立强大的现代合理性结构的基础。

因此，那些寻求传播谎言和谣言的人应该受到谴责，那些在没有证据的情况下推进知识主张的人应该受到质疑。

但公共机构只能做这些了。作为个体，我们可以根据现有证据质疑自己的主观感受。当然，个人经历可以成为有用的知识来源。但我们需要学会区分在个人经验中具有权威性的案例与不具有权威性质的案例。

晚期现代性的条件是我们自然会倾向于依靠我们的主观感受来回答遇到的问题。因此，必须愿意寻求更可靠的知识来源—科学的和道德的来源—来评估自己的冲动和直觉。

这就是为什么与他人（特别是与我们不同的人）的对话如此重要。在追求真实的时代，与我们具有相同主观感受的人可能会判断什么是真实的 —— 因此什么是正确的 —— 就像我们自己一样。这就是为什么我们的社会充满了部落主义。最终，对我们自己来说真实感可以让我们感觉良好，但是，它最终可能不会为我们或社会的最佳利益服务。

真实性不是真理的合适替代品。这就是为什么人们需要生活在自己之外的框架中。

[image]
[image]

我们需要更诚实地思考如何组织

[image] 关键词

[image] 创建时间 2025年1月11日

[image] **Description** 纸条

[image]

[image]

建设中！敬请期待。

[image]
[image]

警惕镇压者通过诈骗在你的设备上安装间谍软件：来自意大利的教训

[image] 关键词	反监视 心理安全 恶意软件 社交工程攻击 间谍软件
[image] 关联	心理安全-PsychologicalSecurity ；[image]匿名手机 ；有针对性的数字监控 ；恶意软件
[image] 创建时间	2026年1月15日
[image] **Description**	纸条

[image]

【NoTrace项目注释】以下消息描述了意大利的无政府主义同志如何被假冒成移动运营商技术人员的社交工程攻击所欺骗，从而在其手机上安装了间谍软件。根据我们的经验及其他同志的经历，我们认为文中所述的攻击：

1. 极可能由国家行为体实施，可能是当地警方或检察机关。

1. 极可能需要移动网络运营商的配合（ [image]移动网络运营商 ）—— 他们会远程切断线路然后再接通，制造手机信号异常的假象，从而为假冒技术人员的干预提供可信度。

此事件应提醒我们：镇压当局的监控能力受限于其财政及其他资源。情报机构或许能获取更精密的间谍软件，实现更隐蔽更可靠的植入；而地方警察和检察机关则可能不得不依赖技术含量较低的手法。

这凸显了在运动内部普及社交工程攻击认知的重要性，以防其他队友

落入此类陷阱。

[image]

可在本站“心理安全”专题中查看抵抗社交工程攻击的一些基本战术和技巧： 心理安全-PsychologicalSecurity

[image]

激进社区用户请从这里进入更多相关内容：[image]匿名手机 ； 有针对性的数字监控 ；以及 恶意软件

我们近期观察到针对政界人士、企业、律师及活动家的间谍软件使用呈上升趋势。我们有理由相信，类似攻击正在被用于调查与反叛运动特定领域相关的个人。

检察官或许更倾向于依赖外部初创企业提供的软件 —— 尽管这些软件都不如Pegasus、Predator、Graphite 或 Triangulation 等高端间谍工具精密昂贵，但仍能执行未经同意收集信息的告密功能。

[image]

返回：[image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击

返回：[image]设备好像被黑了怎么办？ - 数字急救包

返回：[image]如何识别手机上的恶意软件？

返回：[image]S03 变得难以被追踪的简单方法 - 总章节：适合所有理解自由并寻求自由的人

返回：[image]什么是“秘密行动”？政府间谍会怎么折腾你...

[image]

近期部分同志遭遇移动设备入侵事件，过程是这样的：其手机突然无故失去网络及通话功能，所有外拨电话均被转接至运营商总机（或者受害者主动联系了运营商询问原因）。当在与一位工作人员通话后（此人要么表示不知情、要么不了解情况，并报告说可能是连接问题），随即有不同的号码来电，自称是运营商技术人员。

这个所谓的“技术人员”示意目标人的手机“尚未更新”。随后他会耐心细致地指导所有“恢复功能”的步骤，其中包括安装一款带有**SIM**卡运营商名称和标识的应用程序。

安装步骤揭示了该应用的侵入性：

1. 首先，禁用了 Play商店中的 Play Protect 应用分析功能。该功能可保护设备免受潜在有害应用的侵害，确保已安装应用的安全可靠。

1. 随后目标人收到一条短信，其中包含有指向该运营商官网仿冒页面的链接。页面引导用户点击酷似 Google Play 按钮的按钮下载"更新"。

1. 文件绕过Play商店直接下载，用户需在忽略手机所有警告的情况下，从"下载"文件夹中打开该文件。为完成安装，必须修改手机设置允许安装此来源的应用。

1. 之后，手机设置就被更改，允许访问移动网络，从而允许使用运营商的数据连接收发信息。

1. 授予了该应用在后台运行的权限，并允许其在手机开机时自动启动。这使得其即使未在屏幕上显示也能持续运行。

1. 尤其是，授予了该应用所有权限，包括访问相机、麦克风、联系人、电话、短信、日历、位置、文件等等功能。

1. 该应用的电池优化功能已在设置中禁用，因此其活动不会因节

能而受限。

1. 手机重启后，左上角立即出现绿色麦克风图标。随后该图标变为绿色圆点，最终消失。

1. 更令人费解的是，此时居然还收到一条短信，询问："您对我的服务满意吗？"

经过此过程后，很可能所有手机数据（文件、媒体、联系人、消息等）均被此前通过欺骗手段安装的间谍软件应用转发到了远程服务器，使目标人的手机沦为了真正的窃听器 —— 不仅能激活麦克风、摄像头和地理定位功能，还能截取屏幕截图。

鉴于受害者的政治敏感身份及攻击者的技术能力，不难推测此次攻击的来源。因此我们敦促您警惕此类事件 —— 尽管并非所有恶意软件都需用户主动安装（如本案所示），但防范意识仍不可或缺。

IYP 附

请不要认为“这听起来很傻”，“如此高风险的权限要求难道不应该一开始就拒绝吗？”是的应该，但是，如果受害者很孤单身边没有哪怕一个客观视角帮助分析、加之电子设备瘫痪的焦虑、尤其是社交工程攻击者浓厚的伪善层层包裹，为了尽快“恢复功能”，受害者很可能会压制心中的疑惑。

本站“心理安全”专题引言中写道：孤独可能是最大的风险因素，这绝非夸张。

[image] 心理安全-PsychologicalSecurity

对前线社区来说，缓解孤独问题是一项基础性的关键战术。本项目2.0工程将更多讲述这一问题。

在此案的角度上，我们认为有可能通过本地社群内部互助来缓解可能的风险。以下是关于这一构想的部分导图，尚不完整，始终期待更多实践者补充经验。

[image] [image] [image] [image] [image]

以下假设您是协助者，名为**S**：

[image] [image] [image] [image] [image] [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

最后再次提示，对于激进行动者而言，请从 BACK □威胁知识库-索引页 进入，这里收纳了全世界镇压当局最常用的威胁手段和激进行动者多年来积累的防御战术经验。

---

https://www.notrace.how/resources/download/potrebbe-essere-dannoso-installazione-di-spyware-tramite-attacchi-di-ingegneria-sociale-in-italia/it-could-be-harmful-spyware-installation-through-social-engineering-attacks-in-italy-read.pdf
https://www.notrace.how/resources/download/potrebbe-essere-dannoso-installazione-di-spyware-tramite-attacchi-di-ingegneria-sociale-in-italia/it-could-be-harmful-spyware-installation-through-social-engineering-attacks-in-italy-read.pdf

[image]
[image]

转帖：从艾未未回国，反思互联网的“伪”影响和流量魔咒

[image] 关键词	元宇宙 刘小波 影响力 流量密码 监视资本主义 社交媒体 结构革命 艾未未
[image] 关联	[image]S11关系结构革命-总章节；[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？；[image]从组织到行动：极简战术手册
[image] 创建时间	2026年1月17日
[image] **Description**	纸条

由于我们不了解文中提及的个人，以下转帖不完全代表**IYP**意见。

同时表示，我们支持此帖“不针对任何个人”的立场。

[image]

不好意思，接下来我将要说的话也许对不少人来说格外刺耳。但我发誓，绝不/也从不针对任何具体的个人或群体。

很多年来我最经常做的一个评价就是：“有”还是“没有”影响。那么究竟什么才是“影响”呢？这其中可能有着巨大的误解。

基本概念层面上，“影响”指的是：对一个主要事态、局面、趋势，具有作用力 —— 不论是阻止、促进、扭转、还是叠加（叠加是指创建一个齐头并进的竞争性趋势，它能给予“没得选”的人们以新的选择，

类似预示性政治 一个例子 ）。

产生影响的方法有千万种，但其中 唯·独·不·包·含通常情况下被称之为“影响力”的网络流量 —— 流量被视为“影响力”是本世纪最大的骗局，—— 一根胡萝卜诱使全世界老百姓自己逗自己玩从而将自己变成了取之不尽的“人矿”。事实上流量只意味着你帮大厂赚钱的能力、帮条子追捕的能力，也包括外显了自身的平庸指数（流行即平庸这是常识）。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

返回：[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式

换言，这不仅对局势/局面 - 对系统 - 没有任何“影响”，更有，他们实际上是在帮助局势保持进程、帮助系统/体制保持稳固的”耗材“。

同样道理，依靠广告费活着的媒体，不管他们自称有多“独立” 也同样没有“影响”（事实上只是市场媒体，没有被政党绑架而是被金钱利益绑架了，并不“独立”），不论其投资多少、看起来多“敢言”，都没有用，因为它是嫁接在局势之上的，它以·局·势·的·“如·常·进·程”·为·生，并·没·有·对局势产生任何作用力 —— 不论其声称反对还是支持，其本质都是“依附性支持”。

[image] [image]

这是一个魔咒，它让你在生存的欲求与反叛立场的冲突间摇摇欲坠。

无数人曾经试图摆脱它。比如，众所周知的名言“我没有敌人”，其所有含义中就包括看清了这一魔咒后对它的拒绝和否定。但显然，仅仅否定并不足以摆脱它。

于是，有人开始尝试另一种办法，那就是驾驭它。

艾未未就是尝试驾驭这个魔咒的人之一。

是的，他也并没有“直接”对局势本身产生影响（对难民的支持没有能改变难民政策、对加沙的同情也没能阻止住导弹轰炸…），但他的确创建了一个间接的影响，他在一定范围内有效地”影响“了一个庞大的”基数“ - 就如这几天里，他能通过一个小小的新闻访谈”调动“这么多人连续讨论他长达数日，这些人放弃了其他所有更有意义的行动和思考，不假思索地将自己的大部分宝贵时间都放到了那套老生常谈上，慷慨地消耗掉自己的生命光阴，同时坦率地暴露出自己的心理弱点、逻辑错误和眼界狭窄 ……

[image]

为什么说“基数”的有效性并不完全取决于“大小”：云舞白的新生：iyp·整体攻防总述：我们是谁、为何而来 ... 20年战略图谱

这是如何实现的？毫无疑问：“影响”。

我并没有评价这是好还是坏，我说的是：他实现了这一“影响”。我甚至都没有说“这是一种操纵” —— 他确实没有操纵你，真正操纵你的是你自己对流量经济系统/热点逐臭的贪欲。

那么，从战术有效性角度上看，“驾驭魔咒”的方法有什么用吗？的确有。通过创造这个“热点”，他在最大程度上牵制住人群聚焦于一个议题、由此激发出冲突，从而从冲突中“涌现”出更深层的思考 - 从这里开始，便有可能产生真正冲击结构的“影响”。所以我刚描述它为间接战术。

不客气的说很少有人能做到这点。全世界无数网红，99.9%都是廉价的在商言商，本质上不过是脖子上插根草棍跪在那里卖自己。他们是耗材，很可怜，却没有“影响”。不论放到多“大”都不会产生真正的影响；相反，真正有影响的都无法被放大（见下）。而驾驭魔咒者，则是一个介于这两者之间的精准且成功的擦边球。

[image]

延伸：https://iyouport.substack.com/p/--bd1?utm_source=publication-search

但是，驾驭魔咒的方法有着极高的门槛，它不是能普及的 —— 它不仅要求基本面上足够高的知名度和公信力，更要求对局势准确的把控能力、和超出大众的前瞻性，否则就很难用对力气；就像吹哨，吹哨不仅仅是“说出真相”，要想让它具备武器的能力，就必须知道应该在什么时候说、说多少、怎么说（何种形式、面向谁、&战略性的预期部署）。

尤其，更不幸的是，“驾驭”法的持续有效性正在下滑 —— 因为旧的结构正在崩塌，基层已经开始想办法尽快摆脱数字魔咒的绑架、重新形成以“人”为基础的连接 —— 尤其是年轻行动者，果断且坚决；于是很快，这一方法能“影响”到的“基数”大多只是嘴炮而已。

[image]

不过别急，这一方法还剩下最后一点有效性 - 且最后这点价值将持续存在，那就是：

[image]

通过“冲突”，曝光群体的心理弱点，等下 这不是目的！ 真正的目的是 —— 慈悲 ！

慈悲并不是怜悯。慈悲不局限于个人、不执着于个人的言行抉择，

而是 “看到/看清”每个人身后背负的枷锁，进而想办法斩断它 。

这就是为什么我一开始便强调 “不针对任何个人或群体”，我们坐在这里耗费掉这些时间，唯一的目的应该是看清我们自己和彼此的困境，斩断枷锁，解放众人。

如你所见，最后仅剩的这一价值事实上弥足珍贵、无以伦比，然而，要实现它却极为困难，极为极为困难。然一旦实现，它就是一把金钥匙，足以穿透所有历史上失败的革命，开启一扇全新的大门 ……

[image] [image]

□

[image]
[image]

转帖：关于近日再现的街头镇压毒气弹（传闻可能不准）

[image] 关键词	ICE 毒气 镇压武器 防御 防暴武器
[image] 关联	[image]镇压应对措施 ；[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06 ；[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06 ；[image]反击, 保持自由：街头实战指南 S05E17
[image] 创建时间	2026年1月18日
[image] Description	纸条

[image]

为最近几天来再次出现的一个争议补充一些信息：关于镇压现场使用的毒气。每一次镇压行动后都要尽可能确认防暴弹药的成分，这对于救助和调整防御战术来说至关重要。

[image]

返回：https://iyouport.substack.com/p/--06e?utm_source=publication-search

返回：[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06

返回：[image]镇压应对措施

1、

近日明尼阿波利斯市的抗议活动现场再次惊现这种绿色的毒气。和去年底的波特兰一模一样。这种东西在2020年和2021年也大量使用过，传闻认为这是HC毒气。

但究竟是不是HC，暂无定论。

毫无疑问它有毒，它会造成剧烈的疼痛和灼烧感，疼痛和副作用在之后可能会比在当时更加严重。类似这种毒气都含有重金属和铅盐，已知“至少”会导致癌症和出生缺陷。

[image]

2、

任何对局面的“预测”都应该格外谨慎。

在激进行动中，您唯一无法做的事情就是预测局面。局面是瞬息万变的。抗议者既可以因此受益（机动性高）、也可能受损（如果反应不够敏捷或准备不充分的话）。

所以，很建议您多做几手准备。您应该对计划使用的装备非常熟悉和熟练，平日在安全的环境中多练习至关重要。尤其是，别让经验误事。

有经验的活动家经常会声称 “我们完全可以这样这样 …… 因为他们（镇压者）不敢/不会/不可能 做到那样那样”。这可不一定。镇压部队有等级和纪律这没错，这会让他们的常规战术和调动模式相对可预测；但别忘了他们还有绩效，随着紧迫性上升，绩效将高于纪律。

以几个月前波特兰为例，镇压现场格外激烈。催泪瓦斯罐一枚接一枚地发射，弥漫整个街区；到处都是绿色和白色的烟雾。胡椒球被近距离射向抗议者 —— 众所周知这是“违规”的，但他们就是不守规矩，

而你没有办法。联邦特工甚至直接扯掉人们的防护面罩，对着裸脸喷胡椒喷雾。

任何法律维权都是事后的东西，就算咱很幸运能得到事后的“依法赔偿”，咱也得先让自己活到事后才行。如果您选择的面罩太容易被撕掉、或者您觉得自己跑得不够快，那就要小心了 —— 提前想办法提前准备，不能仅仅假设镇压者“不敢/不会”。

3、

传闻普遍认为绿色毒气是HC。这个说法并无恶意，而且是有根据的。这个根据始于2020年。当时联邦特工确实使用了HC毒气，在他们第一次使用HC时他们先部署了一个气罐，然后立即点燃了一枚绿色的烟雾弹，这个烟雾弹在气罐前方引爆。

换句话说，他们是在用绿色烟雾掩盖**HC**毒气，等烟雾散尽后，联邦特工取走了**HC**气罐，而将绿色烟雾弹留在了原地。他们故意让人们误以为绿色烟雾才是被使用的气体。他们不想让任何人知道他们使用了HC。

毫无疑问最后大家还是知道了这一切。但也因此，人们开始将所有情况下观察到的绿色烟雾均视为HC毒气。这可不一定。

请注意：说它不一定是**HC**， 丝毫没有降低它的危险性！ 如上所述 所有这些毒气都有着非常严重的危害，现场的每个人都能证实，还有大量的后遗症接踵而来。

4、

那么，2020年那次是如何确定镇压者使用了HC毒气呢？是通过拍摄气罐燃烧的画面，再将其与之后几晚镇压中使用的气罐进行对比。下面是一个HC燃烧的案例视频。

attachment:91ef81a7-624f-4c74-93ac-e27612d61756:HC燃烧的样

子.mp4

HC毒气燃烧产生的烟雾呈深灰色，有时会略带黄色，具体颜色取决于观察者的 实际观察距离 。 **HC**持续燃烧时，顶部常有 火焰 喷射出，罐体本身高温灼热，在燃烧期间始终呈现明亮的 灼光 。

HC燃放的现场是非常可怕的，浓烟滚滚、能见度极低，每个人都会被厚重的毒气和烟雾包围住，戴着全脸面罩的人会不由自主地把面罩取下来呕吐，而一旦取下面罩，就很可能更快地失去意识，瘫软在地上。如果短时间内没能得到救助，危险性就会快速上升。

毒气会覆盖一个广泛的区域，根本没机会也来不及冲洗。那种情况下只能期待有足够多的街头医生以及尚未晕厥的同伴，快速把失去意识的人拖出污染区。

[image]

返回：[image]警用武器常见伤害及基本处理方法：街头实战指南 S05E06

以下这些照片来自去年6月的一个月内，ICE镇压抗议活动中使用的部分弹药样本。

[image]
[image]
[image]

期待近期在抗议活动现场的朋友提供更多一手的经验和资源。

[image]

返回：[image]反击, 保持自由：街头实战指南 S05E17

[image]

技术哲学和技术直觉-Intuition&PhilosophyofTech

对于安防的目标来说，您不需要读懂代码。就如您不需要拿下土木工程学博学学位也能避免掉进坑里。 技术的底层逻辑是政治哲学，就如万有引力，它解释了任何一种“坑”的危险所在； 他人的前车之鉴绝非笑柄，它揭露了挖坑人的思路和心机。

[image]
[image]

“智能城市”究竟是个什么鬼

[image] 关键词	大规模监视 智能城市 物联网 监视资本主义
[image] 关联	[image]你家冰箱如何作为呈堂证供？
[image] 创建时间	2018年9月5日
[image] Description	技术直觉

如今很多人都知道了，“智能城市”和全方面的侵入性监视之间没什么不同。但究竟被监视的都是些什么内容？要多丰富的数据才能把IBM、谷歌等监视资本主义巨头美成那样？以及我们可以怎么办

- Table of Contents

  智能城市是如何发展的？
  ——运输——
  ——能源和水——
  ——智能健康——
  谁建造和供应智能城市？
  已经建立的智能城市都有哪些？
  ——雅加达——
  ——里约热内卢——
  ——菲律宾——
  ——印度——
  ——中国——

[image]

“智能城市”只是一个营销术语，用于定义技术的使用—— 特别是数据收集技术—— 他们告诉你，这是为了“改善城市的运作”。就像扎克伯格告诉你：“监视资本主义是为了改善服务质量”。智能城市所基于的

理念是，“地方政府对城市居民了解得越多，他们提供的服务就越好”。然而，现实情况是，该营销术语对于从公司到政府的不同参与者来说意味着不同的事物。

世界银行提出了智能城市的两种可能性定义。第一个是“ 技术密集型城市 ，无处不在的传感器和高效的公共服务，这得益于数千个互联设备实时收集的信息。”第二个是“ 一个培养公民和政府之间良好关系的城市 ”—利用现有技术。他们依靠公民的反馈来帮助改善服务提供，并建立收集这些信息的机制。“你信吗？相信政府在全心全意为人民服务？即便是民选政府也应该随时接受人民的监督，而不是寄希望于他们主动正义。权力集中的结果只能是权力滥用。

另一方面，大型科技公司也给出了关于智能城市的定义，例如 IBM 的“城市工作新方式”、或西门子的“ 露天电脑 ”。

智能城市项目的范围从小型初创企业创建的应用程序（例如本地服务级）到非常广泛的基础设施，由 IBM，Oracle 和 Microsoft 等公司设计，集中收集公民数据并提供城市数据分析服务。所有这一切都共同依赖于数据：无论是生成和收集数据还是基于已有数据提供服务。

智能城市是如何发展的？

虽然智能城市极为多样化，但它们最常用于三个部门：运输、能源和健康。看起来没什么要命的？恰恰相反，这三点足够控制住你的整个人生。

——运输——

由英国商业创新与技能部委托编写的一份研究论文将智能交通系统描述为“通过信息收集、存储、操控和随后的传播，为旅行者/客户提供附加价值、引导、提高安全性或效率“。

智能公共交通项目通常很大程度上依赖于“智能卡”。智能卡是旅行通行证，其中集成了电路。这种东西是识别个人身份用的：要么是因为必须以您自己的真实身份注册它们（如巴黎的“ Navigo ”卡），要么是因为它们可以通过其他方式追溯到您的真实身份—例如，需要您使用信用卡充值。

今天，智能城市的发展进一步向“一卡通”迈进了。人们现在可以使用非接触式信用卡或智能手机支付伦敦或北京等城市的公共交通工具，或者以其他形式关联身份，如布宜诺斯艾利斯市的学生证。与系统地收集公共交通数据一样，越来越多的城市也在开发自行车共享计划。中国有什么大家都知道，在纽约，Citibike 一直在分享他们收集的自行车用户数据，从而揭示收集到的数据的范围：旅行持续时间; 开始和停止时间，日期和地点; 性别和用户的出生年份等等一大堆信息。

智能城市也在收集道路使用者的数据，使用电子收费来检测汽车何时开车。

在这样的城市里，你的一举一动都在监视者的掌握之下，你去了哪里、见了谁、持续多长时间等等，显示你的社交关系图谱；你最喜欢去哪里、多久去一次，显示了你的偏好兴趣，这些数据汇总起来就可以全面操纵你了。在这样的地方，汽车和自行车都不再能够帮你逃离危险，反而帮助了追踪你的人。

当中国的共享单车出现时，人们在讨论路权、道德问题等等，是的这没错，但却忽略了其支付方式的危险—— 辅助监视定位的能力，实在不应该。

——能源和水——

能源和水管理技术已经在开始实施了，以优化能源使用并更好地了解需求和供应。能源管理技术的范围从智能电网—由国家实施—到家庭能源管理系统—也称为智能电表。智能电表允许各国获取更多数据，以帮助他们管理储能，并帮助他们解决能量损失和停电的问题。允许公司减少计费错误，并为客户提供更便宜的能源交易。

但是，持续监控您的能源消耗也意味着国家政府、您的能源供应商以及服务供应链中的任何其他第三方，都知道您何时在家、您什么时候醒来，上床睡觉之前是不是喜欢淋浴或泡澡……根据这些数据，可以推断出更多关于你、你的家人和你关系网络中的其他人的情报，例如关于宗教信仰及活动、你家庭的组成等等一切。

这些数据足够做出几万字的社交工程攻击演示。你将遭受什么样的攻击和操纵，取决于你的数据最终落在谁的手里。

——智能健康——

技术和数据收集也被用于让老年人留在自己的房子里而不是搬到养老院去。欧盟是鼓励发展“辅助生活”的机构之一。老年人被要求佩戴可穿戴式皮肤接触设备，将有关其健康的信息（心率、血压等）传递给医疗中心，以便专业人员可以在患者面临风险时立即提供帮助。这些技术还可以检测出可能非自主的人何时离开家、在哪里迷路。放置在房子周围的监视设备能检测到一个人是否摔倒……

在新加坡，作为所谓的“智能国家”计划的一部分，一些老年人的公共管理住宅周围都安装了传感器。这些监视设备能监测到老年人什么时候停止移动，甚至监控他们是不是定时上厕所！

也许你家里有老人，你会担心他们的安全，这完全是可以理解的。但是你有没想过，这些监视数据不是由你—亲人—来掌握的，而是政府部门和技术公司。

如果你被当局瞄准了，他们却无法直接令你妥协的时候，你家老人的一举一动就将变成操控你的杠杆。中国人大多明白这意味着什么，尤其是被当局骚扰过的人。

[image]

谁建造和供应智能城市？

智能城市是公共和私营部门之间合作的结果—— 公司监控伙伴关系的合法化。

虽然智能城市的资金和倡议往往来自地方政府，希望“改善城市”，但国家政府有时可以成为领导其发展的关键力量。例如，在印度，政府启动了一项计划，即“智能城市使命”，在全国范围内开发了100多个智能城市。

此外，地方和国家政府也不是唯一参与这一领域的权力，这种大规模监视的营销参与者还包括欧盟、联合国和世界银行等超国家机构，使用所谓的“利大于弊”的理想化。于是这事儿就严重了。成为了一个已经很难避免的趋势。

更要命的是，无论是中央政府还是地方政府或超国家机构，往往都缺乏内部专业知识和资源，因此他们必须依靠私营部门来设计、实施和维护设备、系统以及基础设施，以促成这些智能城市举措的建立。

然而，公司不仅是推动者和提供者，而且他们也运行他们自己的角色。

虽然提供集成到智能城市的服务的公司多种多样，但值得注意的是，提供数据处理服务的大型企业（如 **IBM**，**Alphabet** 谷歌母公司，微软和甲骨文）如何推动智能城市背后的叙述，这些叙述专注于增加数据的生成、收集和处理。

> **IBM**：IBM 最初创造了“智能城市”这一营销术语。凭借其智能城市挑战计划，该公司已经开发了诸多他们的城市化愿景—基于数据集中化，甚至目标是遍布全球。从那时起，该公司已成为市场中最大的参与者之一，预计到 2020 年其规模将达到近 1.56 万亿美元。

IBM 对“智能城市”的设想是以数据为中心的。根据公司材料，它依靠传感器—能够检测环境变化的电子元件，如温度、运动、光线和声音—放置在整个城市，为市政府的使用创建数据。放置在传输交通流量的高速公路上的摄像机和实时记录水和能源使用的数字仪表（也称为“智能仪表”）是

IBM 提供给当地政府可以使用的数据类型的两个例子。

生成并收集这些数据后，IBM 提供数据分析，以便城市办事处“识别趋势和模式”。然后使用仪表板、可视化和警报在政府机构之间共享信息。

[image] [image]

类似的运营中心现在已经由其他公司在不同城市建立，再现了最初由 IBM 设计的概念。在雅加达，智能城市休息室是一个城市管理空间，包含一个监控室，类似于里约运营中心那样。 这些集中监控室不止收集数据、还会对这些数据进行分析，能在问题发生之前预测问题——就是“少数派报告”的现实版。

[image]

在菲律宾，当市政府与 IBM 签订合同时，总统罗德里戈·杜特尔特（Rodrigo Duterte）的女儿萨拉·杜特尔特（Sara Duterte）自称为该智能城市市长。

在新加坡，政府目前正计划与法国软件公司 DassaultSystèmes 合作创建 Virtual Singapore，以实现“城市仪表板”的下一步。该平台不仅会使用传感器和摄像机汇总来自该市的所有数据，还允许政府官员深入公寓，理由是“分析其能耗并检测可能的气体泄漏情况”。传感器和摄像头将允许政府追踪在新加坡驾驶的每一辆车，并且还允许他们控制人群并进行实验以预测流行病和自然灾害或灾难。政府甚至能够通过监控抓到从高层建筑乱扔垃圾或在禁区内吸烟的人……这些高度侵入性的监控很少能真正实现利他主义。

物联网（IoT）正在改变智能城市的本质。这是连接到互联网的对象的开发和扩展。电脑和手机不再是访问互联网的唯一途径。现在这个监视网络还连接了手表、冰箱、婴儿监视器、电视、甚至牙刷和烤面包机。物联网深深影响了智能城市计划的构思。每个连接对象都成为了当地政府可能利用的数据来源。人们随身携带的手机、有时候是手表都是监视器。在 IBM 对雅加达智能城市的描述中，该公司甚至称将公民称作为“行走的传感器”！

对 IBM 说了很多，主要因为它是这一营销概念的创世者，其他公司

也正在加紧跟上。

> 甲骨文：甲骨文的首要任务是建立一个“有感觉的城市”，一个高度依赖开源智能的城市。他们的宣传册清楚地表明：“甲骨文的智能城市平台提供了收集公民、企业和测量设备等所有类型反馈的方法。数据、测量、消息和事件均来自高科技设备网络，从智能电网中检索，由传统仪器和创新传感器采集。该平台可以自动将这些现实与从社交网络中检索到的更为模糊的信息结合起来。“监视 O2O。

> 日立：日本公司日立现在正专注于智能城市，并一直在收购像 Avrio 和 Pantascene 这样的小公司，以确保他们能够为传感器和视频等智能城市独立提供所有必需技术。

> **Sidewalk Labs**：Sidewalk Labs 是 Google 的母公司 Alphabet 的子公司。2017年10月，他们宣布了重建多伦多12英亩海滨的项目。正如我们早前分析的，谷歌对中国的垂涎并非什么搜索引擎市场，而是智能城市，准确说是庞大的数据。

> 微软：微软依靠与其他公司的合作伙伴关系来提供智能城市基础设施。在印度—该公司正在集中精力创建智能城市和帮助私营公司—他们推出了一项智能城市计划，以赞助有希望在该领域工作的有前途的本地初创企业。

已经建立的智能城市都有哪些？

——雅加达——

雅加达智能城市计划于 2014 年启动，并且是作为 2012 年就开始的更广泛的政府工作的一部分。该市有一系列目标，到 2025 年将实现的目标分为五个类别：智能生活，智能移动，智能治理，智能经济和智能人才。

雅加达智能城市计划非常依赖于一个名为 Qlue 的应用程序—由同名

公司开发。 Qlue 可在手机上提供人们所面临问题的报告：从废物处理到破碎的路灯或者交通拥堵等等。政府使用由印度尼西亚官方谷歌云合作伙伴 TerraLogiq 设计的 CROP 程序回应报告。印度尼西亚政府已委托 IBM 公司来分析公民使用 Qlue 的数据。

但是，**Qlue** 已经成为了监控城市工人潜在负面影响的工具。公民反馈该技术被用来评估城市工人是否有效率（工作是否努力），城市可以在此基础上判断是否解雇工人。仅此一点就留下了滥用的空间，因为恶意者可能会发送大量报告和负面反馈以令员工被解雇—— 就像网络水军利用 Twitter 和 Facebook 的举报功能促使社交媒体封锁异议人士那样。

曾经有报道指，一名 Qlue 用户反复发送多份琐碎事件的报告—污水中的塑料袋、丢失的钢笔等等—以便该分区被显示为一个有问题的地区。后来才知道该用户原来是分区选举的候选人。

——里约热内卢——

里约热内卢 2010 年就成为了 IBM 签约的旗舰城市。IBM 还是警务基础设施的提供商，并为执法目的设计数据分析软件。

智能城市技术—包括 CCTV 交通网络—都集中在城市较富裕的地区。因此，城市管理者更多地在更富裕的地区进行干预—他们从中获取数据—而不是更加贫困的地区，从而加剧了已经存在的不平等。里约行动中心还揭示了建立一个日益受到监管的公共空间的危险，在对指挥与控制综合中心（里约的另一个“控制室”）的工作人员进行采访发现，里约的许多紧迫的社会和安全问题—— 这座城市正在遭遇洪灾和世界杯前的抗议活动，多次遭到暴力镇压。

——菲律宾——

菲律宾的达沃市是另一个案例，智能城市倡议已经导致一个更加苛刻的监视城市的形成。建立运营中心后杜特尔特总统祝贺他的女儿也就是该智能城市市长 Sara Duterte 购买了一套“先进的监控和警务系

统”，其 CCTV 摄像头据称帮助警方抓到了一名达沃商人。 该监视系统的效率已归功于 IBM 的设备支持。

与此同时，达沃市也被目睹了对政治异议的严重压制以及安全部门高度的法外杀戮和滥用行为。罗德里戈·杜特尔特早早已常因其政府骇人听闻的人权记录而受到批评。

——印度——

印度的现实反映了当前对智能城市项目的普遍担忧：这些城市在营销期限之外会是什么样子？这些城市实际上是在为谁服务？

2015 年，莫迪启动了一项计划，在印度建立 100 个智能城市。根据在线媒体 Scroll.in，印度标准局最初试图创建一个可居住指数来评估应该为一个城市提供的服务和基础设施。该委员会设计了包括经济在内的各个部门的指标，教育，能源，环境，健康，治理，运输，住房和安全……对于每个指标，都规定了如何衡量数据的方法。

然而，智能城市举措可能会增加弱势群体被边缘化的现状。例如，据报道，古吉拉特邦的土地被强行收购，用于为富裕的投资者和居民建设智能城市。就像中国发生的事那样，工人阶级社区已经被从中心区迁移出去，街头小贩也被赶出了公路。然而，根据一些报道，正是他们的存在确保了妇女出行更加安全。

——中国——

中国已经成为全球智能城市建设最为积极的国家之一。近年来，智能城市已上升为北京的国家战略，随着政策红利的进一步释放、资金的大量投入，智能城市产业正在变成一块越来越大的肥肉。

2015 年，中兴通讯的智能城市项目就在银川启动：银川市民大厅——这座巨大的、现代化的市民大厅实施全数字化管理，被称为“电子政务的典范、简便市民生活”。该公司给 100 余个中国城市配备了所谓的智能城市技术，整体形成大规模监控。

中兴不仅向超过百个中国城市卖出了智能城市运营平台，也把产品卖到了尼日利亚、加纳和阿尔及利亚等地。法国的马赛和东南亚国家印度尼西亚也是中兴的客户。

去年底，多家美国科技巨头和中国国有企业齐聚深圳参加第十六届中国国际公共安全博览会（简称：安博会）展示大规模监控领域的未来，这些企业都想在全球最大的监控设备市场分一杯羹。

两年前，中国监控市场的规模就达到了64亿美元，政府希望在中国蓬勃发展的技术产业的帮助下，建立一个规模庞大、规模空前的国家监控系统。估计到2020年，中国将安装近三亿个摄像头。中国官方媒体引用的一位“专家”的说法，中国警方在未来几年里将在提升跟踪活动的技术能力上再花
300 亿美元。

> 政府声称他们正在创造智能城市以提供更好的服务质量，然而，如果公众不参与讨论，他们是在为谁制作智能城市？

曾经我们的行为只能在我们在线时被跟踪，而现在我们面对的是永久的监视。

越来越多的监控不仅发生在公共场所，也发生在私人空间，就如新加坡做的那样，无线传感器已经被安装在老人家中，用于监控居民的移动、睡眠模式甚至浴室的使用情况。中国很快也会实施，鉴于中国的老龄化问题，当局有充分的理由这样做。

Blum-Dumontet 在报告“ 智能城市—乌托邦视野，反乌托邦现实 ”中写道：“虽然这些举措有明显的预期积极目标，但它们也具有高度的侵入性，并且很可能会滥用或转向较少利他的目的。”

对于人权记录不佳且没有保护公民数据的法律框架的国家公民来说，思考这些问题尤为重要。“老大哥”效应并不仅限于专制政权。即使在人民有权抗议和组织的民主国家，智能技术也会侵蚀人们的异议能

力。就如在美国和英国发生的事那样。

而且，对智能设施的担忧已经超出了他们可以跟踪我们的行为这一事实。如今人们越多地使用自动化对象取代非自动化对象，就越容易受到恶意软件攻击，数据泄露，勒索软件，物联网僵尸网络拒绝服务攻击。只要你拥有一个操作系统，现在大多数是 Android，iOS 或微软，你就会受到相当常见的攻击形式的影响。

通过智能传感器和摄像头检测市民的一举一动，并收集大量数据，如果这些数据落入恶意者手中、骇客会劫持我们的智能基础设施，那会发生什么？

曾经发生的诸多网络攻击表明，即使是最高科技的基础设施也是如此脆弱。例如，2014 年韩国一家核电厂运营商的计算机系统遭到破坏。虽然当局坚称没有关键数据被泄露，但事件引发了严重的安全恐惧。

如上，所谓的智能城市的趋势很可能已经无法扭转，但技术进步永远不能以剥夺人权为代价。我们需要将个人需求带回城市的核心，当考虑城市化时，需要重点考虑的是解决方案如何影响人们对权利的享受，例如避免歧视的权利，行动自由，隐私，集会或言论自由等。

城市应该为每个人服务而不是为政权服务，为此，决策过程应该是开放、透明和包容的，法律和道德义务涉及所涉及的行为者。各国政府应寻求公民、民间社会以及技术和安全专家、学术界以及私营部门的投入和专业知识。在提出解决方案时，隐私部门应确保进行彻底的问题分析和需求评估，并尊重基本的基础数据保护和安全标准。促进并资助此类举措的其他参与者有责任确保他们这样做。

如果做不到，没有法律保护、没有公民社会揭露，那就必需发动民众一起来抵制这些项目。没有别的办法。

[image]
[image]

小心预览

[image] 关键词	免追踪 渗透测试
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2019年1月23日
[image] **Description**	技术直觉

许多应用程序生成了这些预览而不知道幕后发生了什么。因为在某些情况下，这可能等同于您已经以自己不想要的方式泄露了 IP 地址。

[image]

URL 预览是大多数消息传递应用程序中的一个很好的功能。它们允许您将 URL 粘贴给朋友或同事，并具有您将要查看的网站的微缩视图。

缺点是，许多应用程序生成了这些预览而不知道幕后发生了什么。

因为在某些情况下，这可能等同于您已经以自己不想要的方式泄露了 **IP** 地址。

不要忘了：当您浏览网站时，您的公共 IP 地址会被暴露。除非您使用 Tor 或 VPN 来隐藏它，否则这就是 Internet 的工作原理。

[image]

与消息传递应用程序中的 URL 预览的不同之处在于，您正在向网站所有者广播您正在讨论该网站，而不是仅仅浏览它。

上下文中这种微小而微妙的变化实际上是一个非常重要的区别。你很快就会明白为什么……

几年前，我正在进行一项渗透测试，我尝试在欧洲一家知名公司担任高管。他们拥有我见过的最杰出的首席信息安全官之一，以及一支非常出色的事故响应团队。

在我发送了第一轮钓鱼邮件之后，我正在监视命令和控制服务器，以查找来自用户的连接。

几个小时都没有太多活动，直到我的网络服务器从一个解析回Skype的 IP 地址收到了连接。

这对我来说是一个WTF时刻，因为我的网络钓鱼服务器是全新的，似乎没有一个很好的理由解释为什么会出现这个连接。

几分钟后，又出现了来自另一台 Skype 服务器的另一次点击。现在我真的很想知道发生了什么。

我忽然明白了，有人在 Skype 聊天期间讨论我的命令和控制系统，Skype 正在生成我设置的网络钓鱼站点的预览。我使用自己的 Skype 帐户进行了几次快速测试，果然，我可以轻松地重现这种状况。后来我才知道是事件响应小组在讨论我的钓鱼链接。

但在涉及在线调查、事件响应和运行秘密在线操作时，这种情况会引发更大的问题。

[image]

这里有两个观点：一个是从调查的角度来看，第二个是从你通过网站进行秘密行动的角度来看。

从调查的角度来看，如果您与其他调查员来回传递 URL，最终可能会导致“通知”您的目标您正在谈论他们。这正是我在测试期间发现的，

你可能也不希望这种情况发生。

第二个观点是您运行网站进行隐蔽的在线操作。您可以监控这些网址预览，并确定有人正在讨论您的网站，可能会让您知道您的诡计正在发挥作用，或者您是不是有可能被抓获（同样，上下文非常重要且基于任务）。

无论哪种方式，它都是可以被观察到的一组独特的行为，而不是一般的浏览活动。

我对各种消息传递客户端和服务进行了简单测试。测试只是在 Digital Ocean Droplet 上设置一个 Python Web 服务器（每月5美元计划就足够了）。 Python Web 服务器只打印出连接客户端的 IP 地址和标头。我还设置了特定于此测试的 DNS 记录以便我可以尝试使用IP地址与域名。 WhatsApp 是唯一经过测试的对IP地址和域名响应不同的服务。其他所有服务都很乐意为IP地址生成预览。使用 HTTP 或 HTTPS URL 也没有区别。

以下是调查结果摘要：

Slack：Slack 很高兴生成URL预览并使用以下 User-Agent 标识自己：User-Agent: Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots) 请求的IP地址来自我公开的IP地址，通过我的办公室连接，在移动和桌面版本的 Slack 中。

Apple Messages：Messages 是一个有趣的测试，有一些非常独特的行为。如果您在桌面/笔记本电脑上的 Messages 发布链接，它将直接从您的公共 IP 地址生成预览，如预期的那样。User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0 非常有趣的是你在那里可以看到 Facebot 和 Twitterbot ！

如果您要向目标发送 SMS 网络钓鱼，您可以通过确保您拥有一个名为 apple-touch-icon-precomposed.png 的文件来增强 URL 预览体

验。消息应用程序将在确定可以成功访问目标网页后尝试检索此文件。此文件将用于生成的预览中，并有助于吸引目标点击该链接。它也可以是一种确认 Messages 是首先进行 URL 预览的应用程序的方法。

Wire：很有趣，当您从桌面和移动电话上的应用程序发布 URL 时，您的公共IP地址将显示在日志中。但是，没有显示的 User-Agent 标头。事实上，Wire 发送的唯一标头是：Connection: close 所以这本身很有趣，因为你的许多 HTTP 客户端（浏览器，抓取工具，bots 等）都会发送额外的标头。通过 Wire 后确实变成了“告诉”，也许某人正在 Wire 应用程序中讨论目标站点。

请注意，在 Wire 中，首选项 →选项中有一个设置，名为“为您发送的链接创建预览”。如果禁用此选项，将阻止 **Wire** 执行这些 **URL** 预览。我建议你这样做。感谢 Michael Bazzell 对此提供的帮助。

Facebook：它使用 Facebook 拥有的基础设施来访问该网站进行预览。User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php) 它不使用您的公共IP地址，但确实表明有人在其 Facebook 个人资料上发布了指向目标网站的链接，或者已经通过 Facebook Messenger 发送了该链接。您看到的IP地址将被注册到 Facebook，因此您可以使用 ipintel.io 等网站进行查找。

WhatsApp：WhatsApp 的行为与其他服务有所不同。它不直接预览P地址，但如果您键入域名（和任何端口）它将尝试进行 URL 预览。此外，当您键入目标页面的 URI 时，它会执行连续请求，从而产生大量流量。看起来是这样的：User-Agent: WhatsApp/0.3.1649 N 请求来自您的公共IP地址。

对其他应用来说在粘贴链接或键入 URL 时未生成任何预览或流量。

当然你应该自己测试一下来验证。

您可以采取一些措施来帮助降低风险：

取消 URL — 只是用其他字符替换点和冒号或使用括号的方法。一个例子：

正常是这样：https://www.hunch.ly

改装后是这样：hxxps://www[.]hunch[.]ly

使用安全的VPN - 这是次要的建议，因为它不能缓解原始问题，但对于正在暴露您的公共IP的服务，至少能掩盖。

[image]
[image]

即使数据是匿名的，您的身份仍然可以被识别

[image] 关键词	免追踪 数字足迹
[image] 关联	[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？
[image] 创建时间	2019年3月19日
[image] Description	技术直觉

监视支持者经常宣称这些数据“是匿名的”，不，他们在狡辩。

[image]

由于城市里遍地都是传感器和智能手机，我们所有人都走在一个大型的数据工厂里。通过地铁旋转门、发送文本、甚至只是把电话放在口袋里：我们每小时都在生成位置标记数据。所有这些数据对于想要了解城市的规划者和设计师来说都是一个福音—当然，对于想要了解其中人员的监视资本主义巨头、政府和广告商来说也是如此。

他们一直在高喊着：这些数据是匿名的！已经从数据中清除了任何识别功能！ 但这不是真的。

麻省理工学院的一组科学家和城市规划师在一项新的研究中表明，无论如何，弄清每个人的身份都是相当简单的事。换句话说，当您在城市中处理多个数据集时，可以快速地对匿名数据进行去匿名化。

麻省理工学院 Senseable City Lab 创始人 Carlo Ratti 与 IEEE 共同撰

写了该研究报告。

首先，他们合并了两个新加坡人的匿名数据集，一个是手机日志，另一个是过境旅行，每个都包含“位置标记”，详细说明了每个数据点的时间和地点。

然后他们使用一种算法来匹配数据在每组之间紧密重叠的用户 —— 换句话说，他们有电话日志和具有相似时间和位置标记的过境日志 —— 跟踪这些标记随着时间的推移如何紧密匹配以消除误报。

最后证明，花一个星期的时间可以实现匹配17%的用户、**11**周达到**95**%的准确率 —— 利用智能手机增加的GPS数据，只需不到一周的时间就可以达到这个数字。

虽然麻省理工学院的小组并没有试图揭露这个数据集中的特定用户，但他们证明了恶意者可以使用相同的过程将这些匿名数据集与个人数据集合并，轻松将时间戳固定在一起，以确定每个人的身份。

不仅仅是恶意的个人、政府或公司可以使用这个过程来监视公民。城市规划者和设计师也可以从这些大型城市数据集中学到很多东西 —— 例如，Ratti自己的实验室最近将这些数据用于减少停车的项目，而其他团队则用它来研究从城市贫困程度到可访问性的所有内容—— 需要小心的是，将所有数据合并可以对其进行彻底的去匿名化。

“作为研究人员，我们相信使用大规模数据集可以发现前所未有的关于人类社会和流动性的见解，使我们能够更好地规划城市，”麻省理工学院未来城市交通组织的 Daniel Kondor 在发布中表示。“然而，重要的是要表明识别是否可能，以便人们可以意识到共享移动数据的潜在风险，目前，这些丰富的信息大部分由少数公司和政府机构掌握，他们对关于我们的一切知道的太多了，虽然我们对它们普遍了解甚少。我们需要注意避免数据垄断和滥用。“

换句话说，随着城市规划者、科技公司和政府收集和共享所有人的数据，我们现在必须知道：“它是匿名的”这种宣称绝不是隐私保障。当他们深入研究我们生成的数据时，城市和公民需要要求永远不会被深

入识别这些数据。

[image]
[image]

礼貌的偏执

[image] 关键词	个人 社交工程 防御
[image] 关联	🍎心理安全-PsychologicalSecurity ；[image]信息最小化原则
[image] 创建时间	2019年5月10日
[image] **Description**	技术直觉

“偏执”这个形容词经常被用于贬义。但是，在防止社交工程攻击方面，偏执是一件非常有用的事。你可以在微笑的同时阻止一场致命的攻击。什么是礼貌的偏执？

在防止社交工程攻击方面，偏执是一件非常有用的事。

或者正如雷切尔·托巴克（Rachel Tobac）所说的，“礼貌地偏执狂”—— 你可以在微笑的同时阻止一场致命的攻击。

对于一位前特殊教育老师来说，他承认自己不是技术人员，但是他熟悉渗透所有行业、各种规模公司的最常见攻击媒介。因为单纯的技术保护从来不是那么有效的，操作技术的永远是人，人类是具有天然且顽固漏洞的媒介。

相反，训练有素的人可以成为安全链中最强大的力量—— 人是你的第一道防线。

如果是你不认识的人—— 即使是你认为自己应该知道的人—— 对你特别好，谈论你们之间的共同点和兴趣、或者展示出对你的组织和其他同道的非凡了解和理解，但也必需提醒自己：不该公开的所有信息都是始终不该公开的。

我们都知道善良的人性非常必需和重要，但是，如果善良的人没有注入健康的偏执，那么这些良好的性格特征就很容易被利用。

请注意，友好和礼貌并不一定意味着成为一个傻瓜。

每一个优秀的社交工程师都非常擅长不断进化自己，并且总是在寻找任何他们可以使用的公开信息对目标进行“深度研究”。你在互联网上写下的每一个字都可能构建关于你的超级详细的个人资料。

你家的保姆或者邻居、或者你公司的清洁员，都可能知道关于你的致命信息；一个人在办公室里的照片、戴着徽章的或在照片背景中出现的电脑屏幕，都可以提供大量的信息，任何攻击者都可以利用它来入侵你。

如果我能看到你的电脑，我就可以从托盘中看到你使用的是什么样的防病毒软件。因此，我就可以定制恶意软件并避免在您的计算机上被检测到。

那么，礼貌偏执的最佳方式是什么？

其中一个基础就是，在社交媒体上发布之前进行思考：“如果有人知道了这一点，他们会如何利用这些内容欺骗我？” 这也有助于理解人类行为是如何被利用的。这点很重要，就如 **IYP** 一直强调的：只有当你掌握攻击方法的时候，才能真正学会防御。

劝说/诱导的基本原则包括“互惠、权威和偏好。它们并不复杂，但重要的是要了解它们的工作原理，以及可以如何被利用。

互惠指的是，攻击者会假装主动放弃一些看起来高价值的东西，引诱

你的互惠心理，从而放弃攻击者最想要的东西。

权威指的是，攻击者通过伪装技巧假扮成你心目中的权威，以便可以对你实施操纵 —— 比如你是一名新员工，而对方扮演你的上司，这种时候你很可能难以拒绝他的要求。

如果一个人看起来很好、很巧合地与你拥有足够多的共同点，从而成为了你最好的新朋友—— 请记住，虽然你可能喜欢这个人，但你并不真正“认识”他或她。

避免社交工程攻击的方法其实也不是那么复杂：如果有人声称他们是某人或某种身份，请不要立即相信，使用你能控制的其他不同渠道去确认这点。

不要相信来电显示，篡改来电显示是非常简单的。你只需要记下对方所说的名字和机构名，告诉对方你稍后回拨过去。如果对方是骗子，他们就收不到你的回拨。

专业的渗透测试是最好的办法，尤其是敏感的团队、社区和企业，都应该与专业测试组织合作，他们能帮你发现你自己不了解的安全漏洞。

要知道，社交工程攻击永远不会减少为零。随着预防技巧被不断公开和进行相关培训，攻击者也在关注这些信息，从而制定能避免被识破的升级式攻击方案。

现实不是完美的，但是锻炼防御意识永远都会有效。

[image]
[image]

构建技术直觉：生存在数字世界必备的本能

[image] 关键词	技术直觉 自卫
[image] 创建时间	2019年5月23日
[image] **Description**	技术直觉

[image]

数字世界令人迷茫。它渗透到我们生活的方方面面，但我们很少有人了解它究竟是如何运作的。更糟糕的是，如果我们想让技术为我们工作，很少有人知道应该从哪里开始。

当一些事情变得棘手或令人困惑时，我们不鼓励提问；如果你还没能掌握它，你就是问题所在。这项技术很神奇，构建它的人也是如此。任何无法被理解的技术都会被认为与魔法没什么两样。

如何构建正确类型的知识才能让每个人都能为了自己的目的利用数字世界的能力？在过去十年左右的时间里，这个问题有两个主要答案：

- 为有兴趣学习如何编码的人创造无障碍的机会；
- 将所有这些复杂性外包给少数人，并使这一主导阶级的技能变得异乎寻常。

但我们知道，这些答案都无法解决核心问题。

在过去十年中，我与对战略性采用技术感兴趣的活动家合作。即使是这些拥有最多资源、最明确的政治信仰和最崇高目标的团体也一直在努力建立正确的知识类型，以便做得更好。在选择、管理和使用技术时，按照自己的最佳利益行事并且符合您的政治和偏好是非常困难的—— 有时是不可能的。虽然我长期以来一直认为对硬技能的一次性培训是不可能的，但只是在过去的几年里，我一直致力于明确地针对一种我称之为技术直觉的知识。

我不希望我们的组织合作伙伴学习编码，我希望他们学习如何与开发人员交谈。我不希望他们仅仅是将复杂性外包出去，我希望他们了解他们内部需要的技能，他们可以外包，并且随着时间的推移而调整。我希望他们能够通过他们不一定可以亲自部署的技术发挥创造力，尤其是能够充分理解并以正确的方式表达激动人心的新可能性。我希望他们就技术的失败提出尖锐的问题。我希望他们能够积极地和经常地讨论数据使用可能带来的挑战、以及他们需要做出的负责任地使用数据的决策。

我相信行动中的技术直觉是一种关键的知识形式（不仅仅是技能组合），而且是我们作为一个社会尚且没有充分探索或优化的知识。

目前，让公众广泛参与我们对数字化未来的决策是不可能的。对驱动数字空间创建的知识、权力、基础设施和资源的不对称获取正在推动不平等，政治、经济和社会的不平等。而且，我们过分简化了参与的扩大和对所需技能的获取。我们专注于狭隘的硬技能。但是，像编码这样的硬技能的获得将重新巩固现有的经济关系，而不是重塑它们。

在此之前，我建议我们重新思考自己为积极参与政治和新经济而努力的能力。

- 这不像读写能力。这对系统来说过于被动和顺从。我们不希望系统清晰易读，我们希望它们变得柔韧。

- 这不是次专业。深入理解您在夜间课程中学到的一种编程语言可能会解锁技术领域的工作机会，但这并不能帮助那些想要了解技术而不必将其作为额外技能的人。

- 这也不是关于技术系统对我们做了什么的语话或新闻周期的丑闻曝光。那些东西仅仅能使非技术人员成为观察者的角色。

技术直觉是我们知道和看到但从未努力过的概念框架。这是在技术系统内部和周围广泛探索个性化决策的关键。

技术直觉有四个方面

想象—— 具有信息和本能的想象力，即使没有实施想法的技能，也可以概念化它（这是好的还是坏的）并建议（好的）技术系统；

提问—— 能够提出可以推动理解和决策的问题，以及明确指导这些问题所需的方式和地点（以及专家）；

决定—— 明确您的政治和偏好（个人和专业的）如何与您可以而且应该在数字系统内做出的决策相关联；

要求—— 如果一个系统的设计方式与我们的政治和道德不一致，应该知道什么时候要坚持自己的想法，以及提出要求。

每天都有许多例子和情况，技术直觉可以支持更多的代理和决策。当我们在工作并考虑技术可以帮助我们实现目标的创新方法时，当我们决定如何在线参与时；并且，即使我们只是外出购买杂货，技术直觉也会发挥作用。

我将使用一个几乎普遍的消费者示例来演示技术直觉：我的杂货店建议我注册一张折扣卡，我在结账时要通过扫描以换取折扣。在这种情况下，技术直觉如何发挥作用？

首先想象：该计划产生了哪些数据？这些数据可以说明很多关于我的私人习惯的事，而且完全可以据此对我进行身份识别。它可能用于预测我的行动、我的生活方式（恶习和美德），还可以用于各种其他目的。

商店或那些可能购买该数据的人如何使用这些数据？商店可能会使用它来向我定位广告。也许有一天，他们会根据他们可以告诉我需要的商品或者战略性地向我收取更多费用。保险公司可能想知道我购买了多少酒精或非处方药。信用机构可以使用这些数据来制定关于我的消费习惯的概况或预测。在一些国家，它可能会影响社会信用评分。

数据如何组合使用？如果它与其他公司生成的数据一起使用，那么关于不同购买的多组数据可能会对我有什么影响？以英国的 Nectar 卡为例，它们被用于多个系统，如服务站、地铁站、杂货店和大型商店。

您可能还会想到不同的结果。比如所有数据有一天忽然被公开了会怎么样？对我来说有多重要？对别人来说会有什么用？

其次提问：该计划是否提供有关如何使用数据的任何细节？它与其他公司的计划有关吗？我能节省多少钱？我是否想参与并因此激励该公司实施这一举措？这些省下来的钱是否值得我冒险？对我的家人来说值得吗？会有什么影响？

然后决定：我不会注册那张卡，因为我不认为我交换隐私数据是值得的。或者，我会参加，因为我认为10%的成本降低值得接受这种监视—否则我可能付不起这笔钱。如果是这种情况，也许我会参加，并会偶尔提供虚假的联系方式和与朋友交换卡，以便减少有关我的数据。

再然后，要求：在反思这一举措后，我很惊讶地发现，没有任何关于通过它产生的数据的保护规定，并且商店没有试图清楚地向我解释注册的利弊权衡。如果这是一个让我生气的问题，我会在反馈表中跟进，向当地分公司的工作人员提出。我认识到我对公司的影响力可能远不如政府举措，但我知道消费者保护方面的大多数差距都存在，因为客户没有足够的兴趣和技术直觉来迫使公司变得更好—而政治家对这些问题不够关心，无法保证或激励监管行动。

有许多人致力于开发新形式的复杂性的工具，但通常它们是为那些已经在技术领域工作的人设计的。新工具正致力于提高复杂内容的可解释性; 视觉设计师正在利用用户界面作为技术传授的渠道; 动画师正在努力简约化复杂的技术概念; 公司正在招聘科学传播者; 研究人员正在

研究机器学习论文中的可解释性; 人们正在建立完整的隐喻词典，可以用来解释技术概念。

这项工作令人兴奋—我们应该支持和鼓励它。但我们还需要开发更易于理解的帮助，更清晰地连接概念，并为那些有兴趣了解它们如何组合在一起的人建立一条路径。我们的目标不是每个人都是编码员、统计学家、设计师或工程师的世界，也不是每个人都想成为技术专家的世界。

我们想要一个这样的世界，在这个世界里，我们所有人都可以建立技术直觉，并在数字系统内部和周围重新获得我们的控制权。

如果您正在研究如何支持非技术人员社区发展技术直觉，我很乐意听取您的意见。你在做什么来创造洞察力和理解力？什么类型的见解可以导致更强大的技术直觉？对你的目标受众能有什么影响？欢迎留言。

[image]
[image]

如何使用社交工程来攻击 **2FA**？

[image] 关键词	2FA 社交工程攻击 身份验证 预防性
[image] 关联	[image]如何不暴露手机号、不花钱，实现双因素身份验证？；[image]一次性密码和2FA应用；[image]开源 2FA 应用
[image] 创建时间	2019年8月2日
[image] **Description**	技术直觉

双因素身份认证被认为是相对可靠的保护措施。但是它很可能并没那么安全，使用社交工程伎俩就可以令2FA失败。如何做到的？

- Table of Contents
场景1: 攻击者知道您的用户名和密码
场景2：攻击者没有任何用户数据
抵御
1、
2、
3、

[image]

如今，许多服务都使用双因素身份验证（2FA）来提高用户帐户的安全性。在大多数情况下，2FA 使用密码和通过短信或电子邮件发送的代码作为验证的两个因素。与仅使用密码方法相比，2FA 显著更强、并提供更好的安全性。

但是，2FA 也容易受到攻击。最值得注意的是，攻击者可以使用社交

工程策略绕过2FA并侵入用户帐户。因此，重要的是要充分了解社交工程如何运作以及如何最好地应对社交工程。

作为一名安全专家，您可能已经知道这一点，但您组织中的大多数人可能都不知道。社交工程利用人类行为特征、思维弱点和心理学以实现有效的攻击和入侵。通过使用情绪触发器、以及其他心理策略，攻击者可以说服用户放弃他们的个人信息和其他致命的细节。

正因为社交工程使用的是人类心理学基本特征，所以并没有万无一失的反击方法。几乎没有软件或工具可以有效阻止社交工程攻击。

这就是为什么人类是反对社交工程攻击的第一道也是唯一的防线。如果用户知道社交工程攻击是什么以及如何执行，就更有可能识别它、并且不会因此陷入困境。

反社交工程的第一步是了解它的运作方式。

以下是攻击者可以绕过双因素身份验证的一些最常见的情况。

攻击者使用各种策略来执行社交工程攻击。说到 2FA，两种最常见的社会工程攻击类型遵循下面解释的方案。

场景1: 攻击者知道您的用户名和密码

数据泄漏在当今的数字世界中是很常见的。即使是大公司和在线零售商也会受到影响。在此类数据泄漏期间，大量的用户数据（包括登录用户名和密码）被转储到黑客站点上。

任何攻击者都可以访问这些数据并获取您的登录凭据。但是使用双因素身份验证的话，攻击者就无法仅使用用户名和密码来登录。因此，攻击者会使用社交工程来获取第二步验证的代码。

在这种攻击期间，攻击者可以向用户发送警告消息。此消息说明了以

下内容：如果IP不属于您，则您的用户帐户已从可疑IP地址访问，请使用发送到您的号码的验证码进行回复。

在幕后，攻击者使用您的用户名和密码登录该服务。然后该服务会将验证码发送到您的手机。

如果用户使用验证码响应了那个虚假的警告消息，则攻击者就能够使用它来绕过2FA的第二步。登录后，攻击者还窃取会话 cookie 并对用户帐户进行完全未经授权的访问。

场景2：攻击者没有任何用户数据

现在考虑这种情况。攻击者不知道您的用户名、密码、电话号码或验证码。而且，他仍然可以使用社交工程攻击来获得所有这些信息，以及更多致命信息。

这种类型的攻击使用钓鱼网站—— 伪装成真正网站的虚假网站。网络钓鱼网站通常使用与真实网站十分相似的网址，仅仅差一个字母的区别，例如 Gmaiil. com 而不是 Gmail. com 或 LunkedIn. com 而不是 LinkedIn. com。

攻击者会首先创建一个有说服力的电子邮件，看起来它来自您认识的人或来自服务本身。该电子邮件的链接看起来很真实，并且您被要求登录。一旦您点击该链接，您将被带到虚假网站。

在假网站上，系统会要求您提供登录用户名和密码。当您提供这些详细信息时，攻击者会使用它们在真实的登录网站上登录。真实的网站会向您的号码发送验证码。当您在虚假登录站点上输入此代码时，攻击者也会获取代码并使用它来完成真实网站上的登录。

通过这种方式，攻击者就能够绕过 2FA 并获得对服务或网站上的用户帐户的访问权限。

现在我们已经看到攻击者如何使用社交工程来绕过 2FA，现在是时候

探索可以防止社交工程黑客的一些方法了。使用这些工具和技巧，您可以自己避免社交工程陷阱，并指导工作场所的同事和其他朋友。

抵御

1、

安全密钥是 2FA 中使用的另一种身份验证形式。这些是包含带有一个或多个密码的硬件芯片的物理密钥。这些密码由服务识别，并被接受为身份验证中合法的第二个因素。

安全密钥还具有内置机制，用于在提供存储在其上的密码之前确定网站是否合法。通过这种方式，它们可以防止网络钓鱼网站和虚假登录页面获取用户登录信息。

2、

大多数社交工程策略使用网络钓鱼攻击和会话劫持来获取用户详细信息。高质量的安全 VPN 可以加密数据流量并保护浏览会话。这减少了社交工程攻击的可能性。

VPN 还可以有效抵御针对虚假站点使用 HTTPS 的高级网络钓鱼和社交工程攻击。您必须投资信誉良好的 VPN 才能获得对社交工程的良好保护。这是因为即使是一些著名的 VPN，例如Avast Secureline，也会出现严重的漏洞。

3、

防范意识是对抗社交工程的最重要方式。了解社交工程是什么以及如何工作的用户通常可以更有效地避免社交工程攻击。

组织和团队可以投资于社交工程意识培训，以使其成员能够抵御社交工程攻击。渗透测试和模拟场景是帮助用户了解社交工程如何工作的好方法。

您非常有必要让您身边的人与您保持一致的安全意识和习惯，否则他们中的任何一个人都有可能将您和您的整个团队拉入火坑。

[image]

地主2.0：科技的新食利资本主义

[image] 关键词	技术哲学
[image] 创建时间	2019年10月24日
[image] **Description**	技术直觉

你花了大价钱购买的东西并不真的属于你，你只是个随时有可能卷包滚蛋的租客……

[image]

通过向我们出售硬件但保留软件和数据的所有权，科技公司正在将用户视为数字租户。

当蒂姆库克和他的同事们为苹果公司的活动登台表演时，他们宣布了一个重要的战略支点。

该公司知道其 iPhone、iPad 和 Mac 的市场停滞不前，这一趋势不太可能很快改变。

这意味着 Apple 需要向其客户出售其他产品。

苹果公司在宣布推出一系列需要订阅的新服务后宣称："苹果作为一家服务公司的重塑是真实的：

Apple TV ＋用于播放电影和电视节目；Apple News ＋ 用于汇总新闻出版物；Apple Arcade 用于玩游戏；Apple Card 用于支付所有费

用……

凭借 Apple 庞大的内置用户群，金融分析师估计该公司可能在短短几年内就能达到1亿用户，随着时间的推移创造出“每年**70**亿至**100**亿美元的收入流”。

苹果公司所做的不仅仅是应对竞争压力 —— 而是，它正在跟随技术如何被用来改变财产所有权和利润积累之概念的转变。

Facebook、Uber 和 Netflix 等等都在构建平台并提供服务，努力将自己插入社交关系、经济交易和个人消费。

它们深度渗透到人们的日常活动中，并无止境地收集有关我们行为和兴趣的宝贵数据。

而且，至关重要的是，他们收取访问权费用 —— 而不是所有权，这种模式已经越来越过时了。

然而，所有这些公司正在做的事 —— 包括苹果公司 —— 正在重振长期与地主和封建主义联系在一起的旧形式资本主义幽灵。

无论我们称之为“平台资本主义”、“监视资本主义”，还是仅仅“下一代资本主义”，都没什么不同，这种资本运作模式采用的是调解和封闭来实现对其主体的提取和控制。

“Rentier”是指资产所有者向其他人收取访问该资产的费用的关系，就像房东向租户收取房租一样。

很难低估这种租赁模式现在应用于消费者世界的程度。

近年来，大量企业将自己描述为 “Uber for X” 或 “X as a service” —— “即服务”句式，例如 WeWork 提供“空间即服务”、或亚马逊的 Mechanical Turk 提供“人类即服务”（人类变成投喂机器的流水线工

人）。

风险资本家和企业家正在寻找机会来获取价值 —— 美元和数据 —— 通过控制资产然后向用户收取访问这些资产的费用，无论是办公空间、音乐还是游戏。

除了消费者服务之外，许多政府、企业、大学和其他组织都从平台租用核心服务，例如软件和存储。

这些软件即服务业务现在发生在私人平台的生态系统中，为这些平台提供持续的收入来源，同时巩固了其在经济和社会中的关键地位。

虽然像 Uber 和 Airbnb 这样的例子相当明显，但通过广泛应用的 X-as-a-service 模式，平台也能够以包含日常事物的方式扩展租赁关系。

这里的关键技术是软件许可证，它允许新的租用者声称对嵌入的软件拥有所有权，并且从我们日常生活中使用的越来越多的物理实体中获取数据。

由于物联网概念的崛起，许多曾经普普通通的日用品，如咖啡机和牙刷，现在都配备了软件、传感器和网络连接。所谓的“智能”版本正在成为产品设计和销售的默认方式。

这些软件成为了物品功能的一部分，传感器收集有关物品使用方式的数据，Wi-Fi 将物品连接到公司的平台，以便下载和上传数据。

而且，关键的是，当您购买智能设备时，您拥有的只是物理对象。

数字软件是“许可的”，这只是“租用”的另一个委婉说辞，我们通过使用该东西生成的恒定数据流构成了我们向公司支付的“租金”的一部分。

通过将曾经普通的物体集成到物联网中，这些巨头公司能够制定一种微圈地形式，在这种形式下，它们保留对物理实体的数字部分的所有权 —— 以及访问、控制和关闭软件的权利 —— 即使你“购买”了它。

无论是流媒体内容还是许可软件，我们都在因将控制私有财产的特权转交给公司看门人而付出代价。

数字控制限制你如何使用智能猫砂盒是一回事，但是花30,000美元购买的一辆车甚至花10万美元买的拖拉机似乎就是另一回事了 —— 您拥有的只是一大块金属和橡胶，而实际操作车辆所需的软件你只能租用。

Twitter 上充满了冰箱、门铃和割草机的物联网例子，这些例子都需要互联网连接和常规软件更新才能发挥作用，而这些关键东西总是被互联网霸主掌握，只能等待进一步的指示。

正如 Gizmodo 的 Kashmir Hill 报道的那样，她连接的智能家居中的所有设备都与它们的制造商进行日常联系，不断向他们发送数据并ping更新。

“你购买的智能设备并不属于你；你与制造它的公司分享监护权。”

作为一种封闭技术，软件许可广泛且秘密地成功实现了从“用户”到“所有者”的大规模权利转移。

这就好像你买了一套房子，但你不知道，以前的房东继续拥有厨房；你没有发现，直到他们收回你的厨房，只因为你试图在没有经过他们许可的情况下进行修理或改造。

别忘了，他们一直在监视你如何使用厨房。

考虑一下智能家居的兴起，这种类比看起来并不那么牵强。

平台公司认为自己是服务提供商，而不是数字地主从他们的网络空间或他们的软件飞地中收取租金。但是，无论你叫它什么，也无法改变租借关系的实质。

人们应该将这些新发展置于索取财产、控制权、捕获价值和促进不平等的长期历史中去思考。

地理学家阿利斯泰尔·弗雷泽（Alistair Fraser）创造了“数据掠夺”这一短语，以展示这些当代的圈地动态是如何跟随人类历史上更为暴力的过程的脚步 —— 就如“土地掠夺”。

我们现在看到的食利资本主义的版本正在适应数字时代，但它仍然保持着提取和控制的相同基本特征。

这些租赁者不是通过建筑围栏和收租以获得利润，而是通过使用数字平台和给物理设备安装软件以获取价值。

通过平台业务积累巨额财富的公司告诉你，所有权是一种老式的想法，同时大规模部署了诸如“分享”和“便利”这类诱人的流行语。

但是，他们避免提到访问权的暂时性和掌控权的缺乏 —— 让你同意租用你每天使用的东西。

没有人会希望自己无法掌控自己的全部生活，仅仅作为一个租客。然而，当人们默许或不抵制“提取即服务”的扩展时，这种情况就会发生。

[image]
[image]

你家冰箱如何作为呈堂证供？

[image] 关键词	物联网 监视资本主义
[image] 关联	[image] “智能城市”究竟是个什么鬼
[image] 创建时间	2019年12月20日
[image] Description	技术直觉

当你家冰箱在法庭上指认你撒谎……

- Table of Contents

  问题是什么？
  呈堂证供
  有什么影响？
  信息不对称
  证据的质量和可靠性
  我们是否被允许知道技术在做什么？——
  设备不安全：证据不可靠
  诉诸司法
  自动分析和描绘
  结论

[image]

冰箱只是一个指代。

如今，可以连接到互联网的日常物品和设备已经越来越多 —— 那些被称为物联网（IoT）的玩意，它们在“犯罪现场”中发挥着越来越大的作用，作为执法目标。

你家的电灯、电视、门铃、恒温器、冰箱、微波炉…… 如今都作为了刑事调查和取证的一部分，这一趋势提出了尚未被充分探索的新挑战和风险。

执法部门对物联网的利用，这一讨论必须听取从技术人员到刑事律师、法医专家到民间社会的广泛声音和意见。

隐私国际组织的报告列出了一些初步问题。

问题是什么？

如今这个世界充满了连接互联网的设备和物体。

从家用物品，如门、灯泡、发刷、吸尘器、割草机 ……到可穿戴设备，如手表、Fitbits 和耳机……以及更复杂的物体，如汽车，全部都是联网状态。

这是监视资本主义最肆无忌惮的延伸。

这些所谓的智能物体可以使用传感器、麦克风和相机收集大量的私密数据，这些数据不仅关乎你自己的私密生活，还包括你的家人和朋友的一切。

如下面的Nest恒温器解剖图所示，传感器可以包括温度、湿度、光、超声波、罗盘、加速度计、陀螺仪和GPS接收器…… James Bond 上班时也不会带这么多家伙的。

[image]

人们对这些设备的功能了解甚少，往往没有意识到它们有多么的不安全。

这都不是新鲜事。Barbie在2015年发布的联网智能娃娃就配备了麦克

风、语音识别软件和人工智能，允许儿童用户和玩偶之间的呼叫和响应功能。

挪威消费者委员会于2016年12月发布的报告声明，“在联网设备方面，儿童是特别容易受到攻击的人群”，严重问题包括缺乏安全性、非法用户条款、数据被秘密共享、以及被隐藏营销。

[image]

一个所谓的智能灯泡，仅仅通过收集和分析它关闭和开启的时间规律，就可以掌握你全家的作息规律并识别“特殊行为”。

早在2017年就有报道，Roomba 980 扫地机器人不仅可以吸尘，还同时会向制造商报告房屋的大小和家具的数量。

你我不可能了解遍布在我们周围的各种设备的全部功能，因为像 **Google** 的 **Nest Secure** 中的麦克风一样，它们一直都是保密的。除非被内部人士揭露。

呈堂证供

随着这些设备每天都在激增和渗透，大多数人很少考虑传感器、摄像头和麦克风收集的数据的特定用途意味着什么 —— 意味着政府在刑事调查中寻求和使用这些数据，并将其作为刑事诉讼中的证据。

简单说，你家的生活用品正在作为呈堂证供。

你的冰箱和吸尘器在决定你是不是“有罪”。

在大多数情况下，这些设备*本身*可能不是导致无罪释放或被定罪的关键证据。

更常见的情况可能是，它们将发挥某种作用 —— 引导出其他一些证

据，用于证实或反驳原有的证据，以支持或诋毁证人。

情报机构和执法机构已经开始瞄准这些设备收集的数据；国家安全局（NSA）已经在深入探索联网设备的潜在用途，包括生物医学设备，如心脏起搏器和胰岛素泵 —— 以监测个人。

英国内政部通知隐私国际组织，他们计划开发相关技术和技能，以利用物联网作为刑事调查的一部分。

2017年1月，苏格兰场数字取证主管 Mark Stokes 宣称，“物联网”设备可能会彻底改变犯罪现场调查。

有什么影响？

当检察官在 James Bates 案的刑事调查期间寻求证据时，他们认为这些证据是通过使用亚马逊Echo存储在亚马逊服务器上的 —— 人们已经准备好了对亚马逊的角色发表意见，但很少有人能阐述联网设备作为呈堂证供所存在的问题。

2015年11月，Bates 在他的家里和朋友一起看足球。次日早上，他的一个朋友被发现死在浴缸里。

阿肯色州本顿维尔的警方向亚马逊发出搜查令，要求亚马逊交出嫌疑人家中的 **Echo** 语音助理可能记录下的任何数据。

本顿维尔警方出示了两份搜查令，要求亚马逊提供所有关于 James Bates 的“录音、转录、文本记录和亚马逊 Echo 设备上包含的其他数据”。

当时 Bates 的律师 Kimberly Weber 表示，法院的命令“含糊不清，充满了假设”。

但是当嫌犯自己声称他会自愿将数据交给警方时，争议就结束了。而后亚马逊在同一天晚些时候翻录了录音。

联网设备之危险提出的问题范围包括：数据保护、消费者保护、和阴暗的数据代理行业等等。

知道您所在位置的牙刷、或记录您的睡前活动的智能床垫，这些东西现在都被用于调查和起诉您，与此同时对它们的可靠性完全缺乏公正的审查，并且可能伴随着过时法律程序的挑战。

[image]

信息不对称

在刑事调查中，警察很可能获得比证人、受害者或嫌疑人更多的信息和更好的工具。

在民事诉讼中，通常情况是，一方与另一方相比具有明显的 财务和资源方面的优势，无论是国家还是富有的个人或公司。

这不是与“数字证据”相关的独特问题。

个人通常没有专业知识去分析例如指纹、鞋印、纤维、血液或唾液等物理或生物学证据，同样，他们也没有提取和解释数字证据的技能。

然而，鉴于联网设备本质上所存在的问题，这使得信息不对称非常令人不安。

特别是当你围绕这一问题进行辩论时你会发现，受害者、证人或嫌疑人可能没有意识到他们曾经带入家中或工作环境中的设备所具备的潜在能力。

这些设备一直在记录、处理和传输你我私密生活中大量的信息数据；

设备的所有者可能完全不知道这些设备正在收集、共享和存储哪些数据。

虽然用户可以通过屏幕界面看到一些数据，但是，大量的、特别是发送到第三方服务器（即云存储）的数据，在很大程度上是不可见的。

就如你已经从新闻中广泛看到的那样，例如，一家性玩具公司因未经用户知情而秘密收集私密数据而被起诉。

[image]

作为用户，你不可能知道这些联网设备所生成的全部数据都包括什么，也不会知道服务器收集的数据以及设备本身持续存在的数据都有什么 —— 这些数据都可以通过技术手段被提取。

除非我们具备必要的技能，否则很难获得洞察力；并且，数据保护法的主题访问请求等机制不太可能提供全面的信息。

为了说明这一点，隐私国际组织向亚马逊提出了与 Echo Dot 相关的主题访问请求，想知道设备本身存储的是什么，而不是亚马逊的服务器储存了什么。

亚马逊是这样回答的：

> *“Echo Dot* 设备在本地存储有限数量的数据。虽然我们没有义务向您提供设备本地保存的数据以及我们未处理的数据，但由于您已明确要求，我们可以从您的设备中提取这些少量数据……*”*

就是这样 —— 警察可以访问的内容与受害者、证人或被告能访问的内容之间不仅存在严重的信息不对称，并且，调查或起诉的人员对联网设备的能力也没有足够的了解。

证据的质量和可靠性

警察知道他们自己在做什么吗？—— 很难说。

取证是一个复杂的领域，特别是进行数字取证时，正如我们在移动电话取证方面所强调的那样 ——负责取证的警察很少甚至根本没有接受过专业培训，而他们正在依赖他们基本无法理解的设备给人们定罪。

并且，那些取证设备也几乎没有经过科学的测试，测试被所谓的商业机密挡住了。忽视这些工具的运作方式对刑事司法系统的正常运作是非常危险的。

在法律诉讼的调查阶段，个人可能处于显著的劣势，因为没有任何程度的证据披露。

如果逮捕是基于数字证据，那么，用户可以从他们的设备上获得的信息与警察可以获得的信息之间的不对称是非常明显的 —— 用户认为自己已经删除的内容事实上并没有消失，依旧会被提取出来。

而且，警方不仅更有能力从联网设备的生产商那里获取数据，也能直接从设备中提取数据的工具。

现在警方正在获取更强大的工具，以从更广泛的联网设备中提取、解码和解释数据。例如 Oxygen Forensic Detective 就公开声称“数字助理可作为新的目击证人”：

> *“Oxygen Forensic Detective* 通过工具从移动设备和相关云服务中提取 *Google Home* 数据，为调查人员提供支持。*”*

然而，对易于使用的工具的严重依赖也带来了新的风险。许多人认为这会使数字取证变得愚蠢，并造成误判的重大风险。

Discovery Forensics 的常务董事兼高级法医调查员 Jan Collie 博士告诉上议院科学技术委员会：

> “我在现场看到的是，正规警察正试图成为数字取证分析师，他们正在获得这些相当狡猾的神奇工具，这些工具可以做任何事。 一个普通的警察（尽管他可能是好警察）但他肯定不是数字取证分析师 …… 他们得出结论意味着什么？ 因为他们被迫这样做，他们没有资源或没有经过培训关于如何从这些结果中做出正确的推论。这种情况正在法庭前发生。”

物联网取证可以被视为一种特殊的专业，它根据物联网设备的多功能性和复杂性（如设备差异、专有硬件和软件）可能需要解决多种挑战；跨多个设备和平台的数据；存储数据的专有管辖区等等。

几乎没有人讨论那些没有取证专业知识的人去进行数字取证或从他们获得的数据中得出结论，这存在多大的风险。

这不仅与诸如移动电话之类的复杂设备有关，而且，已经与诸多支持WiFi的门铃之类的廉价联网设备有关。

归因分析就是其中一大风险 —— 这一分析颇具专业性。

归因很难，检查数字证据需要大量的专业知识。最近发生的多起案件都证明了这点。

数据利用造成的信息不对称可能会加剧防御不平等，从而为被告的自卫制造了不可逾越的障碍。

[image]

由于其可扩展性和可访问性，联网设备的数据存储主要在所谓的云中。美国商务部国家标准与技术研究所有一个取证科学云计算计划，旨在提高云取证学的准确性、可靠性、科学有效性和实用性。

他们指出，最棘手的新挑战之一是如何在各种类型的云计算环境中执行数字取证。

例如，数据收集挑战包括在大型分布式和动态系统中定位取证目标；从虚拟机中查找和收集易失性数据等等。

另一个必须考虑的因素是，警方收集的数据所构建的叙述很可能是不完整的，并且很可能集中在一个叙述的部分内容上，这个叙述完全可以煽动某人有罪但忽略了可能使他们无罪的证据。

警方调查人员需要接受严格的培训，如果没有适当的指导和明确的标准，警方就会对不完整的叙述和错误的结论进行刑事调查，从而导致司法不公。

陪审团在不完整的数字证据的基础上做出错误假设的风险已经非常大，特别是当辩方无法确定此类证据是否只是大数据海洋的一部分时。

我们是否被允许知道技术在做什么？——

个人无法获得与警察相同的昂贵技术。

虽然个人可能会被提供所提取的数据以及可能是检察官的专家报告，但是，个人没有自己的取证专家，他们不太可能有能力查询提取过程的严谨性。

并且，正如英国议会科学技术委员会所指出的那样，⚠即使人们拥有资源并试图验证或质疑数字取证专家的结论，一些私营公司也不愿意“披露有关他们自己的开发和测试方法的信息” —— 这意味着许多数字取证方法之正确性的证据基础极其薄弱，或根本不存在。

设备不安全：证据不可靠

访问控制、安全通信和安全存储是物联网环境中的重大挑战。据Motherboard 在2015年的报道，“如果你拥有一个所谓智能的假阳具，就应该假定它已经被入侵了”。

数据通常是在不安全和不稳定的技术基础上生成和处理的；例如，LG Smart 真空吸尘器允许一组研究人员以房屋内部的视角监视实时视频。

设备的设计本身就未考虑到安全性；相反，生产商主要关注的是最小化成本和尺寸。

即使是我们放入体内的设备也没有足够的安全性。美国食品和药物管理局（FDA）不得不召回一堆心脏起搏器，因为它们很容易受到黑客攻击。

[image]

寻求来自联网设备的证据将超越众所周知的产品，例如 Amazon echo 或 Fitbits 等等。

同时，对所谓的物联网的非理性渴望意味着会有过多的设备具有令人毛骨悚然的数据收集能力，同时，也会有越来越多的不安全设备会很容易受到操纵和扭曲。

如果必需在调查中依赖联网设备或以其作为证据，则必需询问有关其提供的“证据”的可靠性的重要问题。

想想看，如果你家的烤面包机含有你并不知道存在的麦克风和摄像头，并且可以通过123的默认管理密码访问……这意味着什么？当被骇客操纵的烤面包机指认你是杀人凶手时，结果会怎样？

现在你必需了解这一风险 —— 每个人都必需了解。因为即便您自己家中没有安置这类恐怖的联网设备，您工作的地方、休闲会所、您出入的大多数公共场所，几乎都存在这类东西。

如果这类设备本身不安全、可以轻松被入侵和操纵，并且入侵的成本很低，那么它们是否可以作为一种证据形式决定一个人是否有罪？这必需怀疑。

但是，显然，了解设备的不安全性也需要技术专业知识。虽然安全系统中的缺陷可能意味着数据已被泄露，但后果可能不会立即显现出来。

从另一个角度来看这个问题，还存在一个与设备的安全性和控制有关的人为因素。家庭成员可能随时使用这些设备，但他们不会意识到设备的控制器可以访问他们的每一次搜索、每一次移动、以及他们的每一个想法。这是当事人很可能无法控制的。

诉诸司法

为了能够将数据转换为证据，人们需要昂贵的设备来解码和分析数据，并且解释这些数据的人必需具备足够的专业知识。

当社会中最贫穷和最脆弱的人被指控犯有严重的罪行时，他们如何支付得起昂贵的专家证据？

他们或许可以在律师的帮助下从设备中寻找原始数据，但是必须由专家向法官或陪审团解释。

如果只有控方可以出示证据，被告怎么能有效地质疑他们知道的证据是不正确的？或者他们根本无法意识到的证据是不正确的？

如果案件中涉及数字证据，就需要获取、询问并理解其重要性。

这需要专业知识。对联网设备的数字证据的来源和完整性缺乏证明性挑战，有可能导致错误的定罪。

此外，司法科学不仅依赖于对相关材料的准确和可重复的检测和分析，而且还依赖于在特定背景下对这些材料的评估性解释。

专家可能不仅需要解释原始数据，还需要解决与设备安全性、被操纵

可能性和证据的一般可靠性有关的诸多问题。

此外，许多设备不仅生成数据，而且公司收集数据并使用它们来分析用户行为并做出推断。⚠如果这些推断也可被用于调查或作为呈堂证供呢？

在诉讼中，如果决定要取消一个人的自由、给他们一个犯罪记录或者处以罚款，就必须有效地审核证据。平等武装原则和对抗性听证权是公平审判权的固有组成部分。这要求每一方都有合理的机会在类似的条件下陈述案情。

包括各方都有机会了解所有提出的证据或提出的意见，以便影响法院的决定。任何限制都应该是在严格意义上合理的，并且应该采取保护措施来保护被告免受这些限制造成的不平衡。

[image]

在涉及 Fitbit 数据的一些广泛被报道的案例中考虑这个问题。

以受害者的 Fitbit 数据为证据，一名男子被指控在康涅狄格州谋杀他的妻子，而在另一起案件中，Fitbit 数据被用来调查一名90岁的老人是否谋杀了他的继女。

在前一案件中，被告告诉警方，2015年12月23日上午9点左右，一对蒙面的袭击者进入了这对夫妇在郊区的住宅，杀死了被告的妻子。

然而，死者的健身追踪应用程序却讲述了一个完全不同的故事。该设备使用数字计步器跟踪佩戴者的步数，根据该设备的数据，受害者在她丈夫说谋杀发生后的一小时时间内依旧在房子周围移动。

但这真的能证明被告撒谎吗？不要忘记数字证据的复杂性。

即使案件正在审判，获取专家证据的能力也不能得到保证，并且取决于司法管辖区以及个人是否可以获得法律援助。

与其他类型的司法科学一样，如果检方可以依赖个人无法获得的专业知识，就注定会对平等武装原则产生影响。

为了在法庭上有用，数字证据通常需要专家的解释。

检察官依赖数字证人的一个众所周知的案例涉及心脏起搏器 —— 个人身体内的联网装置。

一名来自俄亥俄州米德尔敦的男子于2018年1月遭到严重纵火和保险诈骗罪的起诉（据称他烧了自己的住所）。俄亥俄州当局获得并查看了心脏起搏器上记录的数据。为了在法庭上能作为证据使用，心脏病专家必须发表专家声明。监管链证人还有其他问题。

英国议会科学和技术委员会最近的一份报告指出，在许多刑事案件中，司法科学证据至关重要，司法公正取决于该证据的完整性和准确性。

尽管数字取证技术已经迅速增长，但没有可辨别的战略来应对这种情况对刑事司法系统带来的挑战。

该报告警告说，“辩方必须有机会在证据有争议的情况下委托自己的取证检验。”

警察、检察机关和私人资助的客户可以支付的费用，与那些没有钱的底层人相比，存在巨大差异。

在每个司法管辖区内，个人都没有权利获得国家资助的专家。即使他们能获得，由于资金限制，也很可能会影响他们可以获得的专家的类型和质量。

相反，国家总有机会获得丰富的资源，以起诉那些无法支配这些资源的个人，他们没有能力质疑国家的证据或为自己开脱。

自动分析和描绘

数据越来越多地通过自动分析来解释和描述。

公司和政府较少依赖我们提供的数据，而是查看他们自己可以观察、推导和推断的数据。加上机器学习的幽灵，失控甚至疯狂都难以避免。

数据可以说明一个人的几乎一切，并且，通过剖析和机器学习，当局可以掌握模式、预测行为并做出推论，这些都是普通人无法访问的结论。

更不用说以审讯为目的的调查了。无论是存储在设备上的还是存储在所谓云中的，警方都可以访问。

并且，所有技术寡头都根据他们可以访问的数据对您进行了分析。如果这些数据被用作对您定罪的证据，这对您的辩护意味着什么？

[image]

这些形式的分析是否可以被用作证据，严重值得怀疑。

但是，随着被收集的数据越来越多，所进行的分析也越来越多，当局是否会寻求基于用户行为的推论来谴责某人的性格？……

结论

人们不断购买那些能够将数据连接到手机、云端以及相互传输数据的新东西。随着你周围数字间谍的激增，它们制作的数据将不断增加。根据所谓的保守计算，到2020年将有大约250亿台设备被联网。

警方当局从你身边的任何设备中寻找数据，寡头公司开发了易于提取

数据的工具，人们继续购买那些联网产品，却很少考虑这些东西如何背叛你并导致未来的司法不公。

我们急需退一步考虑这个问题，对风险和挑战采取广泛的评估，并为每个人的未来寻求基本保障。

这件事已经非常紧迫了。

[image]
[image]

数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

[image] 关键词	数字取证 移动设备
[image] 关联	[image]数字取证
[image] 创建时间	2020年2月27日
[image] **Description**	技术直觉

如今的人们都知道数字取证是什么东西了 —— 因为已经有太多人因此被抓进监狱、被判刑。但是，数字证据真的靠谱吗？任何人可以信任它作为剥夺一个人后半生的绝对依据吗？本文将展示它有什么问题，并警告自我保护。

Table of Contents

- 信任？
- 证据的准确性：警察知道自己在做什么吗？
- 证据的完整性：技术可以做什么？
- 风险处理缺失：远程访问和网络安全
- 执法部门可以从手机中提取哪些类型的数据？
- 下一步会走向哪里？

[image]

正义的实现取决于社会对证据准确性和完整性的信任。

但是，数字取证领域很难做到这点。

本文以英国为例 —— 仅仅是为例，数字取证正在全球泛滥，它们在各个国家所表现出的问题是几乎完全一样的。

英国法医科学监管机构 Gillian Tulley 将英格兰和威尔士的法医学交付描述为完全不充分的、且已经“在危机之间陷入困境”。

他们这么说是有道理的。该报告发出了与数字证据有关的严厉警告，并且，实话说，目前缺乏应对“数字法证证据迅速增长”的“任何可行战略”。

并且，使用手机提取 [以获取数字证据] 可以说是警察使用的最具侵入性的技术形式 —— 不仅涉及手机用户本人的数据，还涉及曾经与该用户通信的许多其他人的数据。

隐私国际组织（Privacy International）2018年的报告 Digital Stop and Search 中指出，至少从2012年开始，一线警官就一直在使用手机提取工具来获取所有类型的有关犯罪受害者、证人、和嫌疑人的个人数据。

尽管已经有多年的经验，警方可以熟练使用强大的技术来提取、分析和呈现手机中包含的所有形式的数据，但是，这不仅会严重侵犯个人隐私，而且还包含诸多的安全隐患。

更有，这种提取没有任何有意义的规范、缺乏明确其实际具有合法性的依据、迄今未向公众做任何咨询 —— 违背民主程序。

信任？

如果一个民主国家的公民想要“同意“将自己大量的高度私密的数据委托给警察官员，那么，不仅提取的合法性应该清晰易懂，而且，还应该确认数据保护措施具有良好的安全性，并且，还要看到具备清晰可见的专门针对移动电话和数据萃取的详细安全策略和程序。

作为安全风险分析的一部分，公民还需要知道当局在数字提取中使用的是哪些技术，并且需要对这些技术有所了解。

然而，尽管每年对信息安全的威胁都在加剧，而且，显而易见的是，国家网络安全中心一直在强调：“大量数据存储是各种攻击者的诱人目标”，向委员会提供的证据和调查结果表明，关于提取技术的部署以及已有的安全控制措施，存在大量问题。

[image]

数据泄露是由于实施不力或完全没有安全控制而发生的。

在英国，警察部门对于因自己的过错而令人震惊的数据泄露事件并不陌生，他们并已收到了信息专员的多项罚款。

格洛斯特郡警方因泄露了虐待儿童受害者的身份而在2018年被罚款80,000英镑。至于安全控制，北约克郡警察因未能做到数据加密而受到严厉批评。

简单说，民主国家的警察也不能直接信任；民主程序在数字取证领域目前最多只能做到事后批评。

[image]

尽管数据的数量和保留是基本的，但仍然存在更广泛的安全问题。正如 Bruce Schneier 所述：

[image]

“安全是复杂且具有挑战性的。简单的答案无济于事，因为简单的答案总是错误的。您需要的是一种新的思维方式。”

证据的准确性：警察知道自己在做什么吗？

使用手机提取技术的警务人员通常很少接受专业的取证培训，或者根本没有任何培训；并且，他们的工作越来越依赖于他们完全不了解其

功能的设备，尤其是在预算削减和数据量迅速增加的情况下。

[image]

取证专家强调，警方严重依赖于那些易于使用的工具 —— 这些工具通过“按一些按钮” 就能从电话中获取数据，这纯粹是愚弄数字法证学，并且可能破坏真正有意义的检查。

Discovery Forensics 的常务董事兼高级取证调查员 Jan Collie 博士向委员会强调了使用 MPE 技术的人员缺乏取证技能的情况：

> “我在现场看到的是，常规警务人员正试图成为数字取证分析员，因为他们被赋予了这些无所不包的魔术工具，可以执行所有操作，而常规警务人员，尽管他可能会尽职，但是他们不是数字取证分析师……
>
> “正是这些毫无经验的人最终对数据意味着什么做出结论，因为他们被迫这样做； 他们没有资源也没有培训，他们无法从这些结果中做出正确的推断。要知道这些结论会被摆在法庭面前，作为决定一个人生死存亡的关键 。”

严重欺诈办公室（Serious Fraud Office，SFO）向委员会争辩说，随着数字证据在刑事审判中变得越来越普遍，有必要制定更多的法规或遵守商定的标准和规范的机制。

证据的完整性：技术可以做什么？

约克大学的数字取证科学家安格斯·马歇尔（Angus Marshall）和计算机科学家理查德·佩奇（Richard Page）都指出，“我们倾向于依赖第三方工具，我们相信这些工具是根据良好的工程实践生产的；如果考虑使用手机提取，则检查将从内容未知的手机开始，因此，整个取证过程的输入是未知的。

这影响到是否有可能利用所谓的证据来确定哪里出了问题”。

以下是他们的声明：

> “一个工具完全有可能错误地处理输入并产生一些看起来仍然与正确操作一致的东西。在没有客观验证证据的情况下，对工具是否能产生任何结果的正确性方面或其他方面的评估，完全取决于操作员的经验。”

> “还应该记住，就用户而言，硬件和软件的更新可能不会对系统行为产生明显影响，但是，可能会大大改变内部处理和存储数据的方式。”

在美国，美国国家标准技术研究院有一个网络取证项目，旨在向公众提供取证工具的测试报告。

根据 MobileEdit，他们的测试表明，在所有竞争工具中，单个数据类型之间的结果存在显著差异。

每个工具都能够展示出相对于其他工具的某些优势，但是，并没有任何一个工具能够在所有测试类别中都表现出优越性。

[image]

在英国，没有对执法机构购买的设备进行任何测试。正如取证监管者 Gillian Tully 博士所说：“到目前为止，所有那些 [手机提取工具] 尚未全部经过正确的测试……”；“而且不允许对数字取证工具进行逆向工程，因为无论如何这都是非法的。”

为什么会缺乏测试？为什么逆向工程非法？很简单，主要理由就是所谓的商业机密。

正如安格斯·马歇尔（Angus Marshall）向英国专责委员会发表的评论所指出的那样：

“私有技术提供商不愿透露有关他们自己的开发和测试方法的任何信

息，这意味着许多数字取证方法的正确性基础非常薄弱，或根本不存在。”

一家提取公司 Magnet Forensics 直接举例说明了由于缺乏对手机提取工具功能的了解而导致的问题，以至于它们可以做非法的事，但警察没有意识到这一点。

风险处理缺失：远程访问和网络安全

没有被触及的领域之一是：提取技术公司能够远程访问警务人员购买的产品。

此访问权限不仅用于产品更新，而且还用于分析。

Cellebrite 是一家数字取证公司，其 UFED 设备在包括英国在内的世界各地的警察部队中都很受欢迎，该公司在其隐私权政策中指出：

“当您使用 UFED Cloud Analyzer 之类的产品时，如果得到您明确的同意，我们将收集有关 Cellebrite 产品的使用信息，例如您使用该软件执行的提取次数、提取的数据源类型、使用产品时遇到的任何错误、收集的事件数量、使用Web搜寻器的频率、以及使用的视图 ……以上所有数据均称为分析型信息。”

Cellebrite 和其他同类公司都可以远程访问位于警察局内部的设备，从而访问与受害者、证人和嫌疑人的电话相连的工具。而且这个领域是一个黑箱。

此外，由于成千上万部电话被直接插入到这些取证工具中，因此，该工具本身很容易受到网络攻击 —— 例如，它们可能被劫持以发送恶意更新，或者可以提供故意感染了恶意软件的电话进行提取，从而有可能实现入侵警察部门的基础设施。

对于这种攻击形式，可能不是显而易见的或最简单的方法，但坚定的

对手可以尝试所有必要的手段。

执法部门可以从手机中提取哪些类型的数据？

移动设备是一个庞大的敏感数据存储库，可以提供有关其所有者以及用户与之交互的许多其他人的大量信息。

Cellebrite、MSAB 和 Oxygen Forensics 等公司向执法部门出售软件和硬件。将手机连接到这些数字提取工具之一后，设备将提取、分析并显示手机中包含的数据。

这些工具可以提取哪些数据、以及使用哪种方法，将取决于操作系统、安全功能、和电话型号。

隐私国际组织使用 Cellebrite 的 UFED 通过 Physical [ADB Rooted] 提取功能提取了 Android 手机（HTC Desire）以做测试。

下图是警察可能看到的内容的真实示例 —— 他们可以从您的手机中提取的数据。

[image] [image]

下面是从 iPhone SE 提取数据的演示：

[image] [image]

下一步会走向哪里？

随着所有人越来越多的在线生活（手机变得越来越“万能”），个人数据已经迅速变得更有价值。

这些具有显著价值的数据正是警察想要收集、访问和开采的东西，并且也是犯罪分子想要窃取数据的原因。

搜查电话要比搜查房屋更具侵入性，不仅是信息的数量和细节，还有，历史性内容的回溯、以及所有与您相关的所有亲密关系 —— 你甚至无法放在家里的东西全在手机里。

任何当权者都不应无拘无束地获得某人的全部生活，使用手机提取功能需要最严格的保护。

但是，即使合法获得提取权限，也没有任何数据可以做到完全安全。

一旦有人存储了数据，由于事故、粗心大意、内部威胁、或敌对的入侵 ......数据就很容易受到破坏。

处理数据的不良做法，包括对获取数据方式的不了解，都会破坏对严重犯罪的起诉，并导致曝光包含从未被起诉的无辜者的详细信息。

在手机提取的背景下，迫切需要严格的监管以及详细实用的技术标准来确保对这些强大技术部署的公民监督。

在专制国家，人们更应该学会保护自己；开发者应该致力于那些能够保护无辜者免遭数字提取工具侵害的功能。

[image]
[image]

如何从Matrix中醒来

[image] 关键词	变革 宣传 无政府主义 示范 认知 预示政治
[image] 关联	
[image] 创建时间	2020年3月4日
[image] **Description**	技术直觉

只要他们能控制叙述，他们就能控制你的想法；只要他们能控制你的想法，他们就能控制整个世界 ...... 为此，他们构建了一个Matrix。

[image]

在电影《黑客帝国》中，人类生活在反乌托邦时代，被强大的系统囚禁在虚拟世界中。

他们一生都在虚拟仿真中生活，而没有任何方式能知道自己感觉到的东西实际上只是由人为编造的代码构成的。

当前社会的生活几乎与此完全一样。

唯一有所不同的是，让我们在“Matrix”中熟睡的是疯狂的寡头权势，而不是AI。而且它不是代码构成的，而是叙述。

[image]

延伸：https://iyouport.substack.com/p/d6f?utm_source=publication-search

社会是由叙事构成的，就像 Matrix 是由代码构成的。身份、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治、政府 ……它们都是纯粹的精神建构，都是强加于头脑中的精神噪音构成的。

如果我要你指出自己的膝盖，你可以迅速准确地做到；但是，如果我要你指出经济，最接近的可能只是使用一堆语言符号来指向一组概念。为了向我展示经济状况，您必须给我讲一个故事—— 那就是叙事。

[image]

任何曾经经历过片刻精神平静的人都知道，这些都不是您当前实际经验的一部分。

在您的经历中，没有精神、话题、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治或政府，没有关于这些东西的喋喋不休。

你摸不到它们的真实形状，你能感觉到的仅仅是关于“它们是什么”的叙述。

甚至找不到一个“你”，因为事实证明它也是由叙述构成的。

没有心理叙事，没有经历，唯有感觉上的印象出现在没有清晰形状或边界的对象身上。

那种视觉和听觉区域的经历、空气进入和离开呼吸系统的感觉，脚在地面上或椅子上的感觉，那或多或少是总的生活减去叙述所得到的东西。它就是现实。

但是，当您加入精神上的喋喋不休时，所有这些现实都不会再能引起关注。

视觉和听觉领域中的外观突然被划分、并用语言标记，并且对它们的关注仅仅取决于威胁或满足各种议程的人。

你经过了数天、数周、数月或数年的时间，都没有真正注意到呼吸系统或脚在地面上的感觉，因为你的兴趣和注意力完全被吸引到了纯粹是由叙述组成的虚假世界中。

“我足够好吗？我做对了吗？我需要确保完成了所有项目……如果我先做一件事，从长远来看可能会节省一些时间吗？如果我能得到自己想要的东西并实现重要目标，我会感觉很好吗？……税单要到期了。电视上有什么？哦，那些白痴，他们怎么还有脸活着？天哪，我等不及周末了 ……我希望从现在开始一切都按计划进行 ……”

[image]

不断地，不断地。几乎所有的精神能量都进入到这些心理叙事中。

是它们在统治着我们生活的一切。出于这个原因，能够控制这些叙述的人就可以控制我们。

他们已经做到了。

[image]

大多数人都会试图对周围的人施加某种程度的控制。

他们试图通过某种行为和言语来影响家庭家人、社会和就业圈子中其他人的想法。

你的父母长辈以他们自己的经历告诉你如何才能做到 “聪明/才干”，你听到的 “这个世界” 完全是你父亲的心理活动；浪漫的伴侣将被说服他们永远不会分手，因为没有其他人会爱上他们 ……

他们都在不同程度上操纵着个人的叙事。

然后有人发现他们实际上可以发挥自己的能力来影响人们对自己和世界的看法，并将其转化为他们自己的个人利益。

邪教领袖说服追随者为他们服务，终其一生，任劳任怨；

广告商说服消费者相信他们自己有一个问题或不足，只有使用“这个令人兴奋的新产品”才能解决；

雄心勃勃的办公室政治玩家通过在合适的人中赢得青睐并对与之竞争的同伴使用隐秘的破坏行为来攀登公司晋升的阶梯；

记者们知道如何通过推进叙事方式以令他们自己在事业上进一步发展，而此叙事方式必然必需是有利于拥有大型媒体公司的富豪们建立王国的基础……

他们操纵着群体的叙述。

然后就是寡头。最主要的操纵者。

这些现代世界的寡头统治者迅速学到了自文明诞生以来每个统治者都知道的秘密：只要你能控制住一个社会的人们相信某种叙述，你就是那个社会必然的统治者。

身份、语言、礼节、社会角色、见解、意识形态、宗教、种族、哲学、议程、规则、法律、金钱、经济学、工作、等级制度、政治、政府：所有心理结构只会在一定程度上影响社会的信任并获得绝大多数群体的认同。

如果你能对人们所相信的心理构造的事物产生影响，那么你就能对社会产生影响。你就能统治它。

寡头操纵整个社会的叙述。

[image]

这就是为什么在整个人类历史中都存在焚书、异端被烧死、嘲笑皇帝的人被斩首：与主要的叙述不同的观念是关于权力是什么、金钱如何运作、应该由谁负责等等，正是这些 —— 而不是斥责辱骂 —— 在威胁着统治者的权力。

无论何时何地，在任何王国中，人民都可以决定将王官从国王脑袋上取下来，然后将其放在任何普通乞丐的头上，并将其视为新国王。而且这个乞丐将以各种有意义的方式成为新国王。

唯一能阻止这种情况发生的原因是：当时全社会所信仰的占主导地位的叙事，涉及神圣权力、忠诚、效忠、高尚的血统 等等。 将王冠戴在国王头上的唯一支撑就是叙事 。

今天，完全一样的事仍然存在。唯一改变的是公众被灌输的叙事。

人们从学校里、从电视上、从互联网上、从报纸上 ......读到的那些叙述。

人们认为，完全独立于政府的经济是一种行为，其行为取决于消费者的供求关系。但实际上，经济、商业和政府完全由精英阶层的富豪控制，他们也恰好拥有媒体公司，这些媒体公司将有关世界是什么的叙述传播到每个人的屏幕上。

控制经济和商业的叙述，然后控制经济和商业本身。控制关于政治和社会的叙述，然后控制政治和社会。控制者不断将资源分配给寡头，通过这样有效地将社会变成了一个精英阶层的巨型能源农场。

但是，依旧有可能从 Matrix 中醒来。

[image]

这并不容易，而且不会在一夜之间发生。这需要长期的工作。内部工作。和承认被骗的谦卑。

没有人喜欢承认自己被骗了，而我们所有人被欺骗的深度和广度是如此的惊人，以至于很可能会认为只要本地一个独裁者倒台自己就能“自由了”。

支持特朗普的人认为自己“看得清楚”，因为他们能看到贸易战可以威胁到中国经济；而支持北京的人也认为自己“看得清楚”，因为他们能看到特朗普政府的重商主义和霸道 …… 然而这只是一场让全世界都输掉的战争，中美政府是唯一的赢家，无所谓你支持谁。

[image]

延伸：https://iyouport.substack.com/p/e9d?utm_source=publication-search

就如主流的美国自由主义者认为他们“看得清楚”，因为他们可以看到福克斯和特朗普拉扯的宣传矩阵；而主流保守派也认为自己“看得清楚”，因为他们可以看到MSNBC和民主党人勾结的叙述操纵 …… 但两者都可以追溯到同一个木偶大师。

看到这一步仅仅是个开始。

了解您和您认识的每个人在多大程度上被强大的权势人为编程为社会意识的想法所束缚。

不仅在成年生活中，而且自从父母开始教我们如何说话、思考和与世界建立联系以来；不仅在现代世界中，而且还可以追溯古老的曾经，国王和皇后提倡维护社会结构和宗教权力的信仰系统 ……

所有这一切都是为了让所有人对异议免疫，不仅是异议的言论、还包括异议的想法 —— 循规蹈矩的意思就是行尸走肉。

掌权者为了他们的利益塑造了整个社会，要控制住这个社会他们就必须控制住我们所有人以及我们头脑中的所有思想。

自出生开始每个人天然的人格结构已经被过滤掉了并被塑造了，这是为了满足塑造者的利益 —— 而你被告知 “这是为了你好”。

因此，逃离 **Matrix** 必然意味着要成就一个新生。在 **Matrix** 中形成的所有观念、心理习惯和与世界相关的方式，仅在那其中有用。

为了与构成社会基本要素的权力叙述之外的生活重新产生联系，您必须为自己创建一个全新的操作系统，以便独立于旨在让您保持睡眠状态的旧程序，并拿回掌控权。

所以这可能很辛苦。一路上您会犯很多错误，就像重新开始学走路一样。但是，最终，您将无需再任何人进行的编程。

然后，您就可以战斗了。

[image]

返回：

[image]

因为在此过程中的某个时刻，您必然会听到内心深处发出的声音。那个声音告诉你，不仅是寡头操纵者值得愤怒，对所有形式的操纵都应该愤怒。

反对以任何程度操纵他人的人。当眼睛变得敏锐时，操纵的伎俩就像落在白纸上的黑色苍蝇一样引人注目，您的整个系统除了排斥和抵制之外没有其他反应。

这样你就可以开始创作了。从此排斥掉任何试图强行让你认为自己是什么样的人的那些家伙 —— 他们想把你重新拉回 Matrix。

要小心。他们会不断尝试将你拉回去。由于我们的叙述与其他人的叙述如此交织和相互依存，并且与我们的自我意识密不可分；因此，你对 Matrix 的拒绝有可能对您的许多朋友和挚爱构成威胁。

你会发现与他们越来越疏远。但不要怕，因为，你是在有史以来最重要的战斗中战斗。

只要保持清晰的眼光你就不会被情感所误导，不会再次上当。

然后，您想要做的就是拆除那个 Matrix，并将其控制器置于无关紧要的位置。

您将着手以任何可能的方式推倒他们在您的同伴周围建立的操纵牢笼，如果需要的话一个接一个地推倒它们；因为您从自己的经验中知道，我们都有能力让宣传齿轮生锈，让操纵者惊慌失措。

操纵者会反击、会尽一切可能抹黑你，称你为"阴谋论者"、"谣言"，试图让你保持沉默；他们会调用他们所拥有的所有媒体针对您发起抹黑运动，但由于您的眼睛是清晰的，所以这些都不会对你起作用。

是的，他们只有这一种武器，而对您不起作用。

您将开始使用自己拥有的一切技能，从谎言工厂唤醒更多的人，削弱对大众媒体宣传机器的信任，并开拓新的可能性。

[image]

而且，我们不仅会粉碎那些像毛毛虫一样吞噬我们的叙事，而且，还将为自己创造新的叙事，更好的叙事，更健康的叙事。彼此之间，关于世界如何以及我们想要什么。

这是事实：正因为都是叙事，所以一切皆有可能。

与那些同样走出 Matrix 的人联合在一起，你们可以确定社会将如何发展；可以重写规则。它已经开始了。

从失败的宣传机器发出的白噪声中，诞生了一个新世界，一个尊重个人自主权和自决权的世界。

尊重我们进行大规模合作以创建美丽、健康、有用的系统的权利，而不会把一切精力都用来反驳那些顽固地宁愿被奴役的精神病态患者。

[image]

“你永远不可能仅仅通过对抗现有的现实来改变这一切。要改变某些东西，你必须建立一个新的模型，使现有模型过时”— BACK https://iyouport.substack.com/p/23?utm_source=publication-search

从恐惧所浸透的精神错乱的叙述中完全释放出来，让真实世界的真实美感充满您的感官。

当你准备好了，站起来。从此，真正开始。

[image]
[image]

警察和间谍如何解码你的照片？

[image] 关键词	个人 反追踪 开源情报 数字取证 追踪 防御
[image] 关联	[image]社交媒体上的行动主义安全性:框架手册 ；[image]使用社交媒体时你必须注意什么？ —— 更安全的抵抗
[image] 创建时间	2020年5月13日
[image] **Description**	技术直觉

这篇文章是警方取证专家写的。如果您关心数字取证技术，可以下载阅读我们提供过的相关书籍和文档。在物料总站的书籍专题中搜索“取证”。

[image]

只要人类一直在制作图像，我们就可以一直操纵他们。

曾经需要使用复杂的暗室技术来修改图像，但是现在，任何拥有智能手机的人都可以使用免费工具来实现数百种更改。

尽管这对于您的 Instagram feed 来说可能很方便，但它对执法提出了独特的挑战。这意味着：眼见不能为实。

于是警方和政府越来越多地要求图像要由取证专家鉴定，但是，该如何进行、以及走向何方？

[image]

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

激进派社区用户请从这里进入：[image]数字取证

图像识别

目前，分析人员依靠 “图像识别” 的知识来检查和验证图像。

该识别通常分为六个关键区域：

1. 物理的：阴影、照明和反射；

1. 几何的：消失点、图像和3D模型中的距离；

1. 光学的：镜头畸变或像差；

1. 图像传感器：修复了图案噪声和滤色器缺陷；

1. 文件格式：元数据、文件压缩、缩略图和标记；

1. 像素：缩放、裁剪、克隆或重新保存。

我们的调查通常是从看不见的部分开始，而不是可以看到的部分。在这里，我们将重点关注图像中捕获的元数据（上面架构中的第5级）。

文件格式取证：元数据

[image]

激进社区用户请从这里进入：[image]元数据擦除和避免

保存图像时，文件通常包含有关图像的数据，称为元数据。

用于数码相机的可交换图像文件格式中有460多个元数据标签（EXIF 2.3）。该规范可帮助相机使用可以在设备之间交换的格式，例如，确保 iPhone 照片在三星设备上正确显示。

可以包括图像尺寸、位置数据、较小的缩略图、甚至包括相机的品牌和型号等等。

确定哪个相机拍了什么照片

在最近的调查中，我们验证了一组称为 “Byethorne鸭” 的图像。

RSPCA 提供给广告商的图像显示了一只鸭子，头上插着一把刀。很快就出现了指责，有人说该照片是PS的。

[image] *Images of the Byethorne Duck supplied to the RSPCA*

我们使用 Phil Harvey 的 ExifTool 检查了这些图像，并确定其中四幅图像（左侧）是由用一台相机拍摄的，右边的图像是由另一台相机拍摄的。

使用传感器模式噪声和统计方法对此进行了验证。我们使用信号处理滤波器从每个图像中提取了唯一的指纹，并比较了它们彼此之间的相似程度。

较高的值表示它们非常相似并且很可能相关，而较低的值表示它们不相似并且不太可能相关。

当我们比较五个图像指纹中的四个时，获得的值远高于2,000。考虑

到它们之间的相关性，我们可以说这些图像可能来自同一台摄像机。

当我们测试第五张图像时，获得的相似度值接近于零。

[image]

唯一图像ID字段还包含相机固件编号。通过与元数据中还包含的图像和传感器大小进行交叉引用，建议的结论是使用 Samsung Galaxy S7 或 S7 Edge 捕获的前四张图像，使用 Samsung Galaxy S5 捕获的第五张图像。

在元数据中还显示了拍摄图像的时间，从而提供了什么时间拍摄的以及由什么设备拍摄的时间线。

[image] Time the photos were taken and by which camera

由于照片是由两个不同的相机在大约一小时的时间内拍摄的，因此这些图像极不可能是伪造的。

RSPCA发言人证实，它从两个不同的人那里收到了鸭子的图像，与这些调查得出的结论相符。迄今为止，还没有足够的证据确定肇事者的身份。

如何通过普通作品找到一个人的地理位置

相机型号不是唯一可以从元数据中获得的东西。

[image] *A selection of books on the author’s desk*

上图是我在办公桌前拍摄的书籍的图像，从中你可以看到我的办公室在哪里。

[image] Metadata viewed in ExifTool for the bookshelf image

GPS坐标直接嵌入图像元数据中。通过将这些坐标放入谷歌地图，可以显示我办公室的确切位置。

[image]

这种明显的隐私问题就是为什么社交媒体通常会从上传的图像中删除元数据的原因。

图像取证的未来

元数据永远不会孤立使用。

对图像进行身份验证以确保其未被修改，并维护监管链，对警察来说越来越重要。

协助警察的工具可能包括直接内置在相机中的审计日志或插入水印。

我目前正在对以前的研究进行扩展，该研究表明每个图像传感器（实际拍摄图像的电子设备）由于其对光的反应不均匀而具有唯一的指纹。就如 https://web.archive.org/web/20200927134849/https://www.iyouport.org/facebook-%E7%9F%A5%E9%81%93%E5%A6%82%E4%BD%95%E4%BD%BF%E7%94%A8%E7%9B%B8%E6%9C%BA%E9%95%9C%E5%A4%B4%E4%B8%8A%E7%9A%84%E7%81%B0%E5%B0%98%E8%B7%9F%E8%B8%AA%E4%BD%A0/

总之，下次拍摄照片时请考虑一下它可以讲述的故事。

[image]
[image]

你的手机如何背叛了民主？

[image] 关键词	免追踪 操纵 监视资本主义 移动设备 选举政治
[image] 关联	[image]手机应该有且只有一个用途：如何在敌对环境中保护自己S02E03 ；[image]数字技术限制和最佳实践
[image] 创建时间	2020年5月28日
[image] **Description**	技术直觉

2014年（6年前），我的一位朋友在辩论中就这样怒吼："民主都快死了！你们变革能变成什么？我们需要先抓住重点！" 当时没有人能听懂他说的是什么意思。

直到最近两年，一些人开始醒悟。

当然，他所指的远非这篇文章主题所强调的内容，这里只是 一个侧面……

[image]

人们不是不希望保护自己，而是感觉那些真正能起到保护作用的方法"根本不现实"。比如，最基本的保护性措施就是：扔掉你的智能手机。

真话说出来就是这样。而漂亮的假话可以说一大堆。

但是人们依旧想要知道 "如何更改一些设置以缓解灾难"。没错，方法

的确有，只是，可能无法解决根本性问题。

就如 deleteFacebook 运动中很多人寻求的依旧是如何调整隐私设置，而不是如何彻底删除它。

我们已经被绑架了，还患上了斯德哥尔摩综合征，甚至不愿逃离。结果是什么？毁掉民主的就是每个人口袋里的东西。

夜幕降临时，香港的街道几乎到处都是灯光，成千上万的手机被人们举起在头顶摇曳。每一个闪烁都是出席的标志，也是对自由的恳求。

一些抗议者戴着面具以阻止被政府的面部识别监视摄像头网络捕获。

但是，除了明亮的灯光外，每部手机还在黑暗中发出另一个信标 —— 人眼看不见的信标。

有时每分钟多次捕获和收集此信号，不是通过无人机、而是通过智能手机应用程序。在抗议者关掉相机灯、回到家中并脱下口罩之后很久，这些信号一直在广播。

几乎所有国家都会追踪任何将智能手机带到公开示威活动中的示威者，并将目标人在行动中的身影记录在商业数据集中。同时，各政党一直在收集和购买电话位置数据以进行针对性的选民说服。

[image]

返回：[image]当您准备参加抗议活动：基本指南

返回：[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

激进社区用户从这里进入：[image]匿名手机

哥伦比亚大学新闻学教授，60年代著名的激进主义者“学生争取民主社会”组织主席 Todd Gitlin 说：“毫无疑问，这是险恶的。”“这将有效地压制那些宪法声称保护的自由表达。如果人们知道自己会被跟踪，那么肯定会让他们退却。”

Times Opinion 获得了来自超过1200万美国人的电话中的超过**500**亿个位置的大量数据，这有助于说明这种全面监控给公民建立和参与健康民主的权利带来的巨大风险。

无需任何特殊培训，在几分钟之内，只需进行少量的Google搜索，就可以在各个海岸的大型和小型公共示威活动中找出并识别出任何人。

通过跟踪特定的设备，研究人员跟踪了从2017年 Women’s March 大型游行中返回家的所有示威者；并且在2017年就职日 Black Bloc 抗议活动中识别出了每一个参与者。

示威者的匿名性长期以来一直是一个有争议的问题。各国政府普遍不喜欢这个主意，他们声称担心蒙面抗议者更有可能煽动骚乱。

包括纽约州和佐治亚州在内的多个州都制定了禁止在公共示威活动中戴口罩的法律。

包括加拿大和西班牙在内的国家/地区都制定了限制或禁止在所谓的非法聚会中戴口罩的规则。

但是，你必须知道，在智能手机时代 —— 无论是否蒙面 —— 已经没有人能够迷失在茫茫人海中了。

请注意以下噩梦：

- 政府使用位置数据识别重大抗议活动中的政治敌人；
- 检察官或警察使用位置信息以威吓刑事被告进行认罪交易；

- 广告定位技术公司的流氓员工与出于政治动机的团体共享原始数据；

- 大型捐赠者购买了监视定位公司，以帮助增强其政党的政治定位能力，并利用这些信息来压制抗议者；

- 白人至上主义者组织入侵了一家小型企业的不安全服务器，并了解了潜在攻击目标的家乡地址 ……

[image]

返回：🚁空中监视

香港中文大学的活动家，研究员兼教授 Lokman Tsui 告诉我们，出售此数据的第三方是一个问题，因为 “购买此信息的标准非常宽松，公司没有道德审查委员会。我所在的大学就可以购买数据，而且很容易获得。他们可以购买的数据种类让我大为惊讶，“哦，哇，你居然能买到那种东西？”令人毛骨悚然的数据。”

这些数据甚至都不需要泄漏或转手 —— 它的存在本身就已经给民主参与带来令人生畏的影响。

[image]

延伸：https://iyouport.substack.com/p/--310?utm_source=publication-search

话语已经在更专业的抗议者圈子中流传开来 —— 将手机留在家中、将其切换为飞行模式、或仅将其关闭电源（关闭电源没用，除非能把电池抠出来）。

许多反法西斯活动家参加的集会都以掩面为基础，以保护自己的身份免受仇恨团体、警察和新闻界的袭击。“ 我们告诉人们不要将您的手机带到抗议活动中，或者如果您这样做了，请至少保持GPS处于关闭状态……”

[image]

“然而，要知道，您自己越安全，组织起来的能力就越差，” 反法西斯抗议研究员说。

活动家 Joshua Wong 曾协助推动香港2014年雨伞运动，现在是香港持续抗议活动的关键人物。他说，无所不在的追踪从根本上改变了香港的民主抗议活动。

他说：“过去，人们觉得，如果自己不是激进主义者或知名人物，就不会受到监视，因为没什么可隐藏的。但是，他们最近才意识到，随着抗议活动越来越多，监视对所有人构成了严重的威胁，即使他们不引人注目，政府也将其作为攻击目标。”

即使是公开身份参加抗议活动的人，也会对自己的运动被归类到可购买、可出售、可合并、可被黑客入侵的数据库中，而感到不安。

“我个人很高兴向特朗普提出抗议，并让人们知道这一点。但是有很多人说，国家间谍可以仅凭行程模式就可以确定你的身份。老实说，这很可怕”，住在马里兰州 的 Eric Hensal 说，他出现在2016年华盛顿特朗普酒店外示威游行被监控的数据集中。

[image]

延伸：https://web.archive.org/web/20200407143856/https://www.iyouport.org/%E4%B8%8A%E5%B8%9D%E4%B9%8B%E7%9C%BC%EF%BC%9A%E4%B8%80%E4%B8%AA%E6%B2%A1%E6%9C%89%E7%A7%98%E5%AF%86%E7%9A%84%E4%B8%96%E7%95%8C%E6%84%8F%E5%91%B3%E7%9D%80%E4%BB%80%E4%B9%88%EF%BC%9F/

粒度监视仍然是新事物。但是一些专家认为，围绕追踪公民这一问题进行辩论的窗口可能正在关闭。

香港中文大学的 Tsui 辩称，目前中国、美国和欧盟对互联网的构想

存在三种不同模式之间的竞争。

中国正在迅速采取行动，打破包括公民权利在内的一切；以隐私为重点的欧盟正在围绕监视和同意提出道德上的观点。

而美国及其强大的科技公司陷入了困境，一面被抨击道德问题，同时又由于深陷高堡奇人的无意义竞争而担心被中国抛在后面。

[image]

延伸：https://iyouport.substack.com/p/-ai5g?utm_source=publication-search

延伸：https://iyouport.substack.com/p/e9d?utm_source=publication-search

Tsui 说，如果中国向前推进，通过技术消灭人权，美国无疑会紧随其后，那么美国人会发现，使用监视、大数据和人工智能来操纵和改变行为的手段及其直接结果的趋势会直线上升。

[image]

延伸：https://iyouport.substack.com/p/pr?utm_source=publication-search

位置数据已经成为2020年大选竞争的一部分。共和党人和民主党人的政治行动委员会已经在选址数据上进行了大笔的投资，以便根据选民的兴趣来定向操纵。

他们正在招募数据经纪人，以帮助监视那些去教堂的人的动向，以寻找倾向于保守派的选民，并操纵其投票。

在2017年发布的公司文件中，德克萨斯州的一家科技公司 Phunware 将这场竞赛的目的描述为收集针对选民的位置数据，就如 “淘金热”，“只要前几场政治运动意识到以移动广告为定位目标对选民的影

响价值，闸门就会打开。哪些运动会先到达那里并发家致富？”

据报道，该公司与特朗普竞选经理 Brad Parscale 成立的 “美国制造媒体顾问公司”（American Made Media Consultants）签署了一项协议，以提供位置数据收集服务。

Phunware 吹捧选民的智能手机为“最终选民档案”。他们的行销声称，移动数据可以显示目标人的设备 “是使用什么操作系统（**iOS**或 **Android**）以及还安装哪些其他应用程序、设备加入了哪些 **Wi-Fi** 网络 **……** 等等所有信息，甚至更多”。简直如间谍软件一般。

[image]

延伸：https://iyouport.substack.com/p/wi-fi-bf4?utm_source=publication-search

延伸：https://iyouport.substack.com/p/wi-fi?utm_source=publication-search

而且，上述这些甚至还没有包括从中推断出的信息，例如 性别、年龄、生活方式、各种偏好等等。”

当然，这些只是初期。现在发生的许多政治操纵看起来与在适当的时候投放标准的政治广告没有什么不同。但是，未来可能很快就变得一片漆黑。

拥有丰富位置数据的政治候选人可以将其与财务信息和其他个人身份信息结合起来，以建立针对目标的渗透性的心理特征分析，以此操纵和推动选民朝着看不见的方向前进。

[image]

可能的独裁者或专制领导人利用这些数据来误导或分裂选民，并阻止政治敌人在选举日出现在民意测验中。然后，一旦掌权，他们就可以利用他们的大量数据来恐吓激进主义者和抗议者。

那些足够勇敢反叛的人会被跟踪并追踪到他们的家中。至少，他们所有人的名字都被输入黑名单。

[image]

政府监视黑名单上是一种什么样的体验？https://iyouport.substack.com/p/386?utm_source=publication-search

维稳是长期的、隐性的，反对派一旦上了黑名单就很可能再也难以参加现实中的抗议活动；异议将越来越举步维艰。

大数据曾经是营销人员的领域，如今成为了提升独裁者权力的一种手段，任何试图对抗独裁者的尝试都会被其挫败。

换句话说，不难想象由于监视资本主义基础设施而产生的社会控制系统。

“从威权主义和监视相交的例子中可以很明显地看出，我们在世界各地都可以见到的智能镇压状况。隐私权法案是绝对必要的，” 马萨诸塞州参议员 Edward Markey 说，“隐私必须从一开始就被视为一项基本人权。”

麻省理工学院教授 Carlo Ratti 回应了参议员的担忧。他说：“目前的路线是站不住脚的。如果您遭遇对信息控制的不对称，那将非常危险。无论是公司还是国家，他们都可以在反抗者团结起来之前完全压制住政治对手。如果我们走这条路，那将是非常危险且非常不稳定的。”

如果说香港向世界传授了什么，那就是，一旦建立了监视系统，几乎是不可能将其连根拔起的。

维权人士 Wong 先生说，“我认为香港公民担心他们会受到追溯性的监视。随着越来越多的报道显示北京在监视其人民方面的努力和尝试，港人担心他们受到同样的待遇。”

随着时间的流逝，只有那些拥有技术上足以保护自己的手段的人才有权参加抗议，包括拥有第二个一次性电话。

“从技术上讲，匿名是可能的，虽然有点难。现在你只能使用技术来保护自己，因此只有那些有技术能力的人才能做到这一点。但是，隐私并不仅仅是服务于有钱人或极客的。隐私权应该是普世的基本人权。”

即使在非专制国家，不受限制的移动监视的未来也无疑会迫使持不同政见者做出艰难的决定。

“对于反法西斯研究人员和抗议者来说，他们会承担完全暴露的危险。恶劣的状况持续升温。它迫使政府和其他组织之间变得越来越好战。”

全球激进主义者的未来可能越来越像香港。

去年的无领导抗议运动是通过技术实现的。留言板 LIHKG 和诸如 Telegram 之类的加密聊天应用程序使这种组织得以继续进行。

但是，运动本身也被同样的技术所破坏。抗议者使用的一种实时位置跟踪应用程序，用于识别警察的位置，已被苹果的 App Store 删除，这表明政府在资源上将具有竞争优势。

[image]

激进社区用户请从这里进入：[image]数字技术限制和最佳实践

[image]

尽管抗议者戴着口罩，用激光挡住政府摄像机，甚至拆掉可疑的监控路灯柱，但是，每个人口袋里的间谍却在悄悄破坏他们的一切努力。

与我们其他人所有人一样，手机就是你的贴身间谍。

在香港等地，成千上万的手机照亮了天空，这是和平反对权威的表现。但是，只有当这些闪亮的手机最终全部消失的时候，它们希望代表的鼓舞人心的图像和民主精神才能发挥作用。

[image]
[image]

让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

[image] 关键词	反取证 数字取证
[image] 关联	[image]数字取证
[image] 创建时间	2020年7月28日
[image] **Description**	技术直觉

“查手机” 已经过时了吗？如今流行的所谓取证工具旨在满足 “即便不在手机上的东西也能把它搞成罪证”。开发这种取证工具的公司大把，并且没有法律限制其使用方式。是谁正在干这种事？它们有什么能力？

- Table of Contents

  什么是手机提取
  什么是云提取
  这种取证是如何工作的
  用于在移动设备之外获取令牌的工具
  1、Elcomsoft 的 GTEX 工具可以在计算机上搜索身份验证令牌
  2、Cellebrite 的 PC Cloud Collector
  3、UFED Cloud Analyzes 7.6
  4、另一个类似工具是KeyScout，可在PC上查找密码和令牌
  可以获取哪些类型的数据？
  面部识别和云提取
  持续追踪
  结论
  因此提出以下建议：
  取证工具当前支持的云服务列表

[image] 不久前中文网络上流行的一张图

当政府的搜查行为从手机转移到所谓的云端时：云提取技术和 “移动取证的未来” 是什么样的？

手机仍然是执法调查中最常用和最重要的数字资源。然而，警察不仅仅要掌握手机上实际存储的内容，还想要从中了解到目标人曾经访问过什么，主要是通过存储在云中的数据。

Cellebrite 是用于从手机中提取数据的领先监控技术供应商，在其年度趋势调查中指出，在所有调查中大约一半证据都 “出现” 了云数据，并且 “通常” 涉及社交媒体或应用程序 —— 那些并不在物理设备上的数据。

数据 “不驻留在物理设备上” 表示执法部门正在转向 “云提取”：对存储在第三方服务器上的用户数据进行取证分析，那些通常由设备和应用程序制造商备份的数据。

然而，随着执法部门越来越多地将云提取用于从应用程序中获取数据，大众对此的警惕性完全没有跟上节奏。YouGov 的一项调查显示，在英国，有45.6%的人没有考虑过手机上应用程序创建的数据存储在哪里，而44.3%的人完全不知道或不认为他们手机上的应用程序使用云存储。

[image]

随着人们花更多的时间使用社交媒体、消息收发应用、使用 Dropbox 和 Google Drive 之类的东西来存储文件 …… 随着电话变得更加安全、锁定的设备更难以破解，并且基于文件的加密变得越来越普遍 …… 正如一位著名的业内人士所言，“可以说云提取决定了移动取证的未来。”

> “基于私有云的数据代表了取证调查人员挖掘潜在证据的虚拟金矿。”

隐私国际组织从取证学角度反复提出了对手机提取风险的担忧，并强

调了缺乏有效的隐私和安全保护措施的危险。云提取则将风险更进了一步 —— 它不仅可以访问手机中包含的内容，还可以访问目标人在其中使用过的任何内容。

[image]

您的手机具有可供开发的所有数据，已经成为解锁在线个人和职业生活的万能钥匙。

需要更大的紧迫性来应对这种提取所带来的风险，尤其是，当考虑到在分析提取数据的软件中增加面部识别和情感识别时。

国家部署了哪些新的监视技术并没有告知公众、缺乏清晰易懂的法律框架、政府缺乏可辨别的行动，几乎没有减少公众免受数据利用的危险。

对高度敏感的数据采用这种狂野西部的做法只会带来滥用、误用和错误审批的风险。这对被控严重罪行的受害者尤其不利，特别是，我们甚至缺乏执法部门提供的有关他们在做什么的基本信息。

云提取技术的部署几乎没有透明度，而且是在公众了解非常有限的背景下进行的：本报告将隐私国际组织的开源研究、技术分析和信息自由法案的结果汇总在一起，以尝试揭露这一新出现的对人权的紧急威胁。

什么是手机提取

手机提取工具是允许警察从手机下载数据的设备和软件，包括：

- 联系人
- 通话数据 —— 你打电话给谁、何时通话、以及持续多长时间

- 短信
- 存储的文件 —— 照片、视频、音频文件、文档等
- 应用程序数据 —— 你使用什么应用程序、以及存储在其中的数据
- 位置数据 —— 近乎实时的跟踪
- Wi-fi 网络连接 —— 可以显示您连接到 wi-fi 的任何地方的位置，例如曾经访问过的工作场所和居所

移动电话提取需要与要分析的目标移动设备建立物理连接，以提取、分析并显示电话中包含的数据。

但是，它不仅可以提供设备本身所包含的内容，而且还可以成为通向云和外部信息源的入口。如果警察从检查的目标设备中提取登录名、密码和令牌，就可以使用它们来验证凭据以提取云存储的数据。

什么是云提取

云提取（或云分析）是一种访问、提取、分析、和保留存储在云中的数据的能力，这是技术公司广泛使用的术语，通常是指从第三方公司的服务器上提取。示例包括
Dropbox、Slack、Instagram、Twitter、Facebook、Google 产品如 My Activity、还有 Uber
和 Hotmail 等。

随着云存储越来越多地用于社交媒体、与互联网连接的设备和应用程序，云提取为挖掘大量敏感个人信息打开了大门。

在有关基于云的数据爆炸的相关报告中，有数据显示到2025年，将有

49%的数据存储在公有云环境中。思科全球云指数预测了全球数据中心和基于云的IP流量的增长，并预测到2021年公有云数据中心的使用将继续大幅增加。

- BACK https://steemit.com/internet/@iyouport/7jsklp

[image]

> “来自移动应用程序的大部分数据都存储在云中。这意味着有大量的用户数据可用于收集。”

例如，Cellebrite 的 UFED Cloud Analyzer 使用可以从设备中提取的登录凭据然后从 **Google** 网络历史记录中提取搜索历史、访问过的页面、语音搜索记录和翻译记录，并查看在 **iOS** 设备上使用 **Chrome** 和 **Safari** 进行的文本搜索在 **iCloud** 中的备份。

通过获取登录凭据，即使目标人不再拥有这部手机，它仍然可以继续跟踪目标人的在线行为。

[image]

这种取证是如何工作的

有多种方法可以 “绕开移动设备的状态或配置” 访问云数据，这从取证的角度来看很有吸引力。

第一种涉及应用由个人提供的已知用户凭证，即 当个人自愿提交其登录详细信息时。第二种是从电话中提取数据，然后使用在该设备上或在其他设备（如笔记本电脑）上找到的令牌，用户可能在其中通过浏览器保存了身份验证令牌。第三种方法涉及在公共领域中收集数据。

> “当用户成功通过应用或云服务进行身份验证时，该服务会返回一个令牌，该令牌用于使用户无需再次输入用户名和密码即可访问该服务。令牌就像一个通行证，例如当您打开 *Gmail* 帐户并使用它登录时不需要您进行任何交互。大多数令牌在身份验证时都设置

了有效期限，这会因应用程序或云服务器而异。有些仅适用于单次登陆，另一些则适用于两个星期，还有一些适用于*30*天，如果用户在同一移动设备上使用该应用程序，则永久有效。

令牌的使用避免了登录时触发的双因素身份验证（2FA），后者通常会阻止对数据的访问。

在2FA中，提示用户确认发送到独立设备（例如 移动电话）的代码的过程是一项关键的安全功能。但是，即使触发了 **2FA**，**Oxygen Forensics Cloud Extractor** 仍可以通知政府间谍，并且 “提供了多个选项来绕开附加步骤。”

用于在移动设备之外获取令牌的工具

1、**Elcomsoft** 的 **GTEX** 工具可以在计算机上搜索身份验证令牌

“如果用户的计算机上安装了 Google Chrome 浏览器，并且用户通过浏览器登录了至少一项 Google 服务，就可以对 Google 帐户进行无密码身份验证。

新的 Google 令牌提取器（GTEX）工具会自动在用户计算机上搜索由 Google Chrome 浏览器保存的身份验证令牌。

用户在浏览器中登录自己的 Google 帐户后，这些令牌可实现对 Google 服务的无缝访问，而无需重新输入密码。”

2、**Cellebrite** 的 **PC Cloud Collector**

“是一个独立的工具，可以使用浏览器中的 Cookie 和该PC上安装的应用程序从目标PC上创建令牌。”

3、UFED Cloud Analyzes 7.6

“扩展了其密码收集器功能，以包括保存在移动网络浏览器中的密码。审查员现在可以使用密码收集器从各个站点检索密码登录信息，以收集有关嫌疑人或受害者的最大数据量。这是通过利用用户访问在线帐户时保存在浏览器中的登录详细信息来实现的。”

4、另一个类似工具是KeyScout，可在PC上查找密码和令牌

“ KeyScout 安装了闪存卡并从 Windows PC 收集凭据。然后可以将收集到的凭据导入 Oxygen Forensic Cloud Extractor 中，以立即使用。”

[image]

这些取证工具不仅提供了一种访问云存储数据的简单方法，而且还提供了比个人使用自己的用户名和密码可以访问的更多的数据。

例如，Elcomsoft 称：“即使可以使用正确的身份验证凭据（例如 用户名和密码），也无法访问存储在云中的证据。”

Elcomsoft 将使用 Elcomsoft Phone Breaker 可获得的数据量与不使用取证工具时可获得的数据进行了比较。他们认为，使用取证工具不仅简单快捷，而且可以访问云中的数据，甚至比知道用户名和密码时获得的信息更多。

报告表明，还有其他方法可以使用令牌访问基于云的帐户。

2019年7月，《金融时报》报道称，NSO 集团臭名昭著的 Pegasus 恶意软件可以通过复制受感染手机的身份验证密钥来进行云提取，从而允许单独的服务器模拟手机及其位置。

- [image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击

[image]

尽管诸如亚马逊、苹果、谷歌和微软等寡头公司评论了英国《金融时报》在NSO Group上的报道，但仍不清楚这些寡头在执法部门使用的云提取技术方面的立场。

谷歌告诉英国《金融时报》，与 Pegasus 有关的技术 “没有证据表明它可以访问 Google 帐户或系统”。但是，鉴于有很多取证公司公开宣传对 **Google** 产品的访问权限，因此您必须意识到，这对于客户数据的安全性而言是一个重大威胁。

可以获取哪些类型的数据？

监视公司关于通过云提取可以访问哪些数据类型的宣称令人印象深刻。

例如，Cellebrite 的 Cloud Analyser 声称 “使用司法鉴定程序提取、保存和分析所有公共领域和私人社交媒体数据、即时消息、文件存储、网页和其他基于云的内容”。

这包括一整套 Google 产品。而仅凭其 “历史记录” 功能就可以：

“通过从 **Google** 网络历史记录中提取文本搜索、被访问的页面、语音搜索记录、和翻译的历史记录，并在支持 **iCloud** 的 **iOS** 设备上使用 **Chrome** 和 **Safari** 进行文本搜索，从而洞察目标人的意图和兴趣。”
—— Cellebrite

取证专家声称能够获取未送达的消息、未接听的电话、有关从私人和群组聊天中删除的消息、帐户所有者和联系人的个人资料图片和状态消息、回复中嵌入的原始消息以及广播消息。

简单说，数据不仅与目标用户有关，而且还与他们的朋友、家人、同事、及与之交互的任何人有关。

下图显示了 Cellebrite 对可以从手机中提取的数据量与可以从云来源中提取的数据量的比较，显示了与社交媒体、电子邮件、文件共享、以及位置和搜索历史有关的更多信息。

尤其是使用 Google 带有时间戳的位置记录、以及 Google My Activity 数据和备份来 “按分钟显示实时位置信息、搜索和访问过的网站”。

[image] [image]

Oxygen Forensics Detective 取证分析工具的开发公司称可以从 “最受欢迎的云服务” 中获取数据，包括 WhatsApp，iCloud，Google，Microsoft，Mi Cloud，华为，三星，电子邮件（IMAP）服务器等。

> “还支持各种社交媒体服务，包括并不限于：*Facebook*，*Twitter*，*Instagram*等。… 在撰写本文时，它支持 ***54***种不同类型的云服务 ，从文件存储到 *Messenger*、无人机、健康应用程序和社交媒体。*”*

即使您使用端到端加密消息传递，一旦将WhatsApp消息备份到了云，执法部门仍然可以访问它们。

[image]

Magnet Forensics 还提供了一种云提取服务 AXIOM Cloud，它 “支持9个父级服务中的大约25个云产品，其中包括 Apple Box，Dropbox，IMAP / POP，Facebook，Google，Instagram，Microsoft 和 Twitter 等。每个服务都细分为不同的子服务。”

通过查看可以更详细提取的数据类型，Cellebrite 的 Cloud Analyzer 产品更新显示了对来自 **Alexa** 和 **Google Home** 等智能设备的数据的需求不断增长。

Cellebrite 的 UFED Cloud Analyzer 7.2 “提供对包括音频在内的用户

请求的访问”。

正如 Cellebrite 所说：

> “物联网（IoT）创造了更多使用数据的方式，使我们的生活更轻松，并且它也创造了更多的数字情报来源，供调查人员在进行刑事调查时使用。”——Cellebrite

请注意 Cellebrite 并不是唯一一家促进家庭智能助理访问数据的移动提取公司。Oxygen Forensics 同样将数字助理视为新的目击者，这些设备估计用户数量到2021年将达到18亿：

> “提取的宝贵数据可以包含大量信息，其中例如：帐户和设备详细信息，联系人，用户活动，传入和传出消息，日历，通知，用户创建的列表，创建/安装的功能，首选项等。
>
> 该软件的一项惊人功能是能够提取用户提供给 *Alexa* 的存储语音命令。用户的真实声音！
>
> 毫无疑问，从亚马逊提取的信息将为用户的日常活动、他们的联系人、共享的消息、以及有价值的语音命令提供深刻的见解。”
>
> “当 *Alexa*用户说出唤醒词来执行一项查询功能时，查询记录就会发送到该用户的 *Amazon* 云帐户。 政府间谍可以提取 ***Amazon Alexa*** 数据，以包含用户实际话语的这些有价值的音频记录 。”

随着连接到互联网并因此将数据存储在云中的设备数量的持续增长，云提取不仅可以进入人们的家中，甚至还可以进入人们的身体 —— 从可穿戴设备中访问数据。

- BACK https://iyouport.substack.com/p/cdc?utm_source=publication-search

“从 Fitbit 到 Apple Watch，当今的许多用户都在使用健康可穿戴设备，其中的数据包括心率、位置、食物摄入量、消息传递等信息，这些信息通常仅在云服务上而不在移动设备上。”

Cellebrite 可以访问 Fitbit “用户个人资料、日志、活动、目标、朋友关系、心率、运动轨迹（速度，位置，时间等）。

[image]

UFED Cloud Analyzer 7.3 访问 Google 位置数据和 Booking.com 的“用户个人资料、购买历史、消息和搜索”，这是与旅行和位置有关的另一种数据来源，UFED Cloud Analyzer 7.6 支持从 **UBER App** 中提取数据，并且可以：

“获得乘客和驾驶员资料数据、上下车的位置记录、以及用户信用卡的后4位 ...

检索信用卡详细信息，新用户必须在首次登录时填写此信息。当乘客选择了接送地点、期望的目的地、和可用的驾驶员时，每次旅行都有详细记录。记录的路线经过汇总，然后按常用的目的地进行分类。驾驶员的信息包括姓名和证件照片。”
—— Cellebrite

考虑到 Amazon 和 Facebook 的流行，这些显然是云存储数据的目标。截至2018年第四季度，Facebook 每月有23.2亿活跃用户。亚马逊在2017年拥有3亿用户。

Cellebrite 的 UFED Cloud Analyzer 7.5 的更新包括：“五种全新功能，可访问[针对 Facebook] 的活动日志、搜索历史、主页、用户群组数据、和IP地址记录。”

该软件可以：

> “ …从标记了嫌疑人的帖子和照片中提取信息，以寻找新的线索或新的嫌疑人。
>
> 其他数据点包括识别点赞页面或将某人添加为朋友时建立的连接，以及发布的评论、阅读的文章、观看的视频、参观的地点等等。
>
> 对于群组和页面上的用户数据，*UFED Cloud Analyzer 7.5* 还可以标记嫌疑人是否是某个页面或群组的成员或管理员。
>
> 此版本还可以显示 *Facebook* 日志*IP*地址记录， 以使监视者能够识别用于访问帐户的手机或计算机的位置。”

UFED Cloud Analyzer 7.5 “可以访问[Amazon]的搜索历史、购买历史和送货地址，这些信息可以为政府间谍提供重要的数字证据。”

“在此版本中，您还可以查看在亚马逊帐户中注册的信用卡的后四位数字，包括账单和送货地址。” “随着时间的推移，买家的搜索历史记录和愿望清单可能表明哪些可疑行为导致了犯罪。”

云提取技术还可以从无人机中访问数据，例如 UFED Cloud Analyzer 7.6，其中添加了 DJI Drone App 和 SkyPixel 社交网络。它：

> “允许监视者访问该应用程序以及 *SkyPixel* 社交网络上的相应用户帐户；用户个人资料数据和存储的无人机飞行日志数据都是可检索的，包括：日期、距离、飞行时间、位置、视频和图像。 *SkyPixel* 用户个人资料还可以帮助监视者验证是否对特定视频以及跟踪标签、关注对象等进行了任何协作。”

随着越来越多的公司依靠云存储来开展与工作有关的活动，可以从设备上的令牌获得的可访问数据不仅与个人生活有关，而且还包括他们的工作。例如：“ Cellebrite 提供了从 Slack（商业社区流行的通信工

具）访问共享文件和即时消息数据的权限。”

UFED Cloud Analyzer 7.9 还包括对 Snapchat 和 Instagram 增强功能的支持。当我们考虑以下内置于分析软件中的不断增长的面部识别功能时，这是有意义的，该分析软件可以分析从手机提取的数据以及通过云提取获得的数据。

[image]

面部识别和云提取

使用云提取技术从手机和其他设备提取的数据分析越来越多地包括面部识别功能的使用。

如果我们考虑可以从包含面部图像的 Instagram、Google照片、iCloud 等基于云的资源中获取大量个人数据的现实，那么在大量数据上使用面部识别的能力就很重要。

毫无疑问，它可能被用于大量的云存储数据而没有任何透明度和问责制。

早在**2017**年**8**月，Cellebrite 为其分析平台引入了所谓的“先进机器学习技术”，该技术可用于分析从云中提取的数据，其中包括面部识别和匹配。

从2019年7月开始，Oxygen Forensic Detective 内置的 Oxygen Forensics JetEngine 模块提供了对人脸进行分类的功能。

Oxygen 不仅可以在提取的数据中提供面部的分类和匹配，而且面部分析还可以基于性别、种族、和情绪识别进行分类。

Oxygen首席运营官 Lee Reiber 表示，该工具可以“在证据集中搜寻特定的面孔，或将同一个人的图像聚合在一起。还可以按种族或年龄

组以及“喜悦”和“愤怒”等情绪来过滤面孔。

[image]

持续追踪

获得用户的凭据后，不仅可以获取其基于云的数据，还可以使用其基于云的帐户来跟踪他们。

例如，Cellebrite 的 Cloud Analyzer 的功能就包括：

“跟踪在线行为，分析帖子、点赞、事件和联系，以更好地了解嫌疑人或受害者的兴趣、人际关系、观点和日常活动。”

这提供了对个人生活的非常侵入性的了解。个人本身永远不会知道有人可以访问并正在使用他们的云数据。

[image]

短期或长期的活动监视（特别是没有手机或在设备之外时）这非常具有侵犯性，并为云提取功能带来了另一个令人担忧的方面。

监视者不仅可以随时通过其登录凭据或访问其基于云的帐户的功能来跟踪和监视目标人的行为、消息和位置数据，而且还可以发送消息，模仿目标人，将包含非法内容的信息发送给其他人。

结论

由于没有有关使用云提取技术的详细信息，因此不清楚这是否合法，也不清楚如何保护个人免受滥用其数据的危害。（我们会坚持建议您尽可能不要使用云）

可以从云服务中提取的数据量，包括分析图像的面部识别技术，即使仅提取与一个人有关的云数据，也将产生获得更大量周边人的个人数据的影响，足以表明这种技术应该有更大的透明度和责任感。

这是执法机构的危险趋势的一部分，希望在全球范围内确保其使用的新技术形式的透明度和问责制。

以下是隐私国际组织的建议。

搜索一个人的基于云的数据比搜索他们的家更具侵入性，不仅是信息的数量和详细程度，还有可回溯性和继续挖掘未来数据的能力。 当权者不应无拘无束地获得公民的全部生活，使用云提取需要最严格的保护。

因此提出以下建议：

1、对警察和边境部门对云提取技术的使用加强独立调查；征询公众、民间社会、工业界的意见。

2、在对任何基于云的数据进行取证检查或以其他方式访问其中存储的任何内容或通信数据之前，警察必须获得法官基于合理怀疑而签发的逮捕令。

3、必须有明确的法律依据来检查、收集、存储和分析基于云的服务中的数据，必须提供足够的保障以确保仅在必要且相称时才使用这种侵入式权力。

4、必须发布针对公众的权利及其提取内容的指南，并将其提供给要对其设备进行分析的人员。

5、必须告知目标人其基于云的数据已被提取、分析和保留。

6、检查过基于云的数据的任何人都应该可以使用有效的补救措施，

从而可以提出有关合法性的任何担忧。

7、执法人员必须对合法使用这些权力的遵守情况接受独立监督。

8、网络安全标准应达成共识并分发，规定必须如何存储数据、将其保留多长时间、何时必须删除数据，以及谁可以访问它。

9、使用这些权力的所有主管部门都必须通过公共领域的采购渠道购买相关取证工具，并定期更新其已购买工具的清单，包括有关所拥有工具、制造商、和支出金额的详细信息。

10、创建并遵循技术标准以确保进行验证和确认。例如，这应该伴随有明确记录的过程。

11、需要足够的技术技能。因为拥有如此空前的数据量，必需由具备高技能的取证调查员来执行。

12、云提取技术的测试、试验和部署必须伴随准确的评估、适当的保障措施、以及公众和民间社会的参与。

取证工具当前支持的云服务列表

[image] [image] [image] [image] [image]

[image]
[image]

警察查手机的东西长什么样？——从技术角度看移动设备取证

[image] 关键词	个人 反取证 取证 威胁识别 移动设备 防御 预防性
[image] 关联	[image]数字取证
[image] 创建时间	2020年8月21日
[image] **Description**	技术直觉

这是一个不断快速发展的领域，因为设备和功能的变更很快。但目前为止它已经足够危险，于是，人们必须至少了解它能做到什么、如何做的，才能有希望开启公正的辩论。

- Table of Contents

  对手机提取技术的一般说明
  Android 和 **iOS**
  漏洞
  分析：访问和提取：物理、逻辑、文件系统
  逻辑提取
  它是如何工作的？
  利用漏洞
  解锁 **iPhones**
  文件系统提取
  它是如何工作的？
  利用漏洞
  物理提取
  它是如何工作的
  iOS挑战
  Android – Using vulnerabilities：紧急下载模式

分析：对提取的数据进行分析
结论

[image]

本文将引用公开获取的信息以及 “隐私国际” 组织使用 Cellebrite UFED Touch 2 进行手机提取的经验，来研究移动设备取证技术。

始终欢迎该领域专家的意见。明显的，这是一个快速发展的领域。即便手机制造商宣布了新的“安全功能”，提取数据的技术也能找到新的方法来绕过限制。

对手机提取技术的一般说明

移动电话提取技术（也称为移动取证）需要与目标设备进行物理连接。就是警察把您叫到警局里去用的那个东西。

虽然取证专家、黑客和销售间谍软件的任何人都能够访问和提取数据 —— 甚至可以远程做到这件事，但本文仅着眼于将其产品出售给执法部门的最知名的商业公司，例如 **Cellebrite**、**Oxygen Forensic Detective** 和 **MSAB**。

Android 和 iOS

在研究提取技术时，我们的分析重点是 Android 和 iOS。 Android 是全球领先的手机操作系统，“根据IDC的数据，在2017年第一季度，Android 占据了整个行业85%的市场份额。”

iOS在安全性方面处于领先地位，并提出了最大的法证挑战。“ …没有密码，我们几乎无法从现代iOS设备中提取任何东西。”

例如，iOS 的USB受限模式（最早出现在iOS 11.4.1中）在最后一次解

锁一小时后禁用USB通信，这会阻碍进行数据提取。

随着iOS发行版中USB限制模式的发展，对于取证界的许多人来说，这仅仅是要克服的挑战。

这不奇怪，移动电话提取技术完全可以被描述为军备竞赛，供应商不断寻求克服手机安全性增加的障碍。

在取证功能方面，iOS 和 Android 之间的一个重要区别是，Apple 可以直接向用户推送更新、修补漏洞，而 Android 用户主要依靠制造商和运营商来提供更新。这导致许多 Android 手机运行的是较早版本的操作系统，也就是说，意味着各种形式的提取都是可行的。各种各样的操作系统版本和使用它们的硬件平台提供了广泛的数据提取方法。

漏洞

在评估 MPE 技术时，该项目着眼于一些用于获取数据的漏洞，尤其是对于 Android 手机而言，例如对具有高通芯片组的设备使用紧急下载模式。

当前警察都使用哪些技术来访问、提取和分析手机中的数据？

> “移动设备取证可能是数字取证领域曾经或将要看到的最迅速发展的学科，主要是因为实际设备的环境瞬息万变。设备操作系统每一天都在变得更加先进，并且当前设备上的存储容量是天文数字。当今的设备是移动计算平台，但是访问这些设备中包含的数据比从任何其他数字设备访问数据都要困难得多。”

访问手机和提取数据并不是什么新鲜事。但是，随着每个人手机上数据量的爆炸式增长、以及“移动设备景观日新月异”，访问、提取和分析这些数据的能力变得越来越困难和复杂。

从芯片组（高通，联发科技）到操作系统版本，提取技术会因手机的

硬件和软件而异。从移动设备提取数据是成功的一半。操作系统、安全功能和智能手机的类型将决定您对数据的访问量。”

加密和其他安全措施也带来了重大挑战。

> “随着移动技术的不断成熟以及安全性和加密技术的不断增强，知道如何在受密码保护的智能手机上访问数据变得越来越困难。”

有三种通用的提取类型：逻辑、文件系统和物理 —— 这提供了一种考虑提取技术的框架。

没有单独一种技术可以访问和提取所有电话中的所有数据，并且不能保证一种提取方法能够成功。

正如手机取证公司 MobilEdit 所承认的那样，在评论美国国家标准技术研究院（NIST）用于移动设备获取的测试结果时：

> “在经过测试的竞争工具中，各个数据类型之间的结果存在显著差异。每个工具都能够展示出相对于其他工具的某些优势，并且没有一个工具能够在所有测试类别中都表现出优越性。我们的结论是，执行交叉引用工具分析时，成功率显著提高。在现实世界中，当有案件时，每一项证据都很重要。结合使用多种工具，您可以获得高达***89.6***%的总体成功率。”

物理采集通常是首选方法。它从设备存储中以二进制形式提取原始数据。即使有可能，也存在一种观点，即“应该始终获得逻辑采集，因为它可能仅包含解析的数据并提供检查原始内存映像的指针。”

诸如移动设备的状态之类的因素将确定是尝试逻辑提取还是物理提取。

> “检查的类型取决于设备的电源状态以及设备是否被

> 锁定、是否受密码保护还是被禁用（拆卸或损坏）…并非所有移动设备都可以进行物理提取。例如，*iPhone 5 ～ X* 无法使用非侵入性方法进行物理提取”。

进行手机提取的现实情况是，提取者会经常不得不尝试使用该工具提供的所有类型的提取。但是，执行此操作的能力将受到时间、资源和专业知识的限制。

[image]

云提取是一个发展中的领域，也更危险，值得警惕 [image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

由于掌握了保存在远程服务器中的内容，并且没有数字取证技能的人都可以访问，并可以花钱买到完全抓取的一键式的技术，这种发展尤其令人不安。

云提取是从手机上的内容到可访问所有内容的飞跃，它是对加密和设备锁定的一种反应，这些加密和设备锁定使传统手机取证变得困难甚至不可能，然而却对存储在云中的任何信息量做出了完全的响应。以下是文件内容：

> “当今的数字调查人员不应忽略存储在各种云服务中的数据的重要性。云数据非常重要，从传统来源（例如移动设备、闪存介质或计算机）收集的信息是有限的，不确定的或根本无法获得的。”

提取数据后，就会提供一些令人印象深刻的产品来读取和分析提取的数据。这些产品越来越多地具有人工智能功能以协助取证人员。

分析：访问和提取：物理、逻辑、文件系统

首先分析提取的三种主要类型：逻辑、文件系统和物理以及用于执行提取的工具。这些方法的技术性以及它们可以提取的数据的类型和数

量各不相同。

[image]

如 Magnet Forensics（下图）中的幻灯片所示，可以通过 iTunes / ADB 备份或安装代理来实现逻辑提取。使用特权访问（例如 root 或越狱）的文件系统；和物理使用恢复或引导加载程序的方法。

[image]

还有其他侵入性方法可以从电话中提取数据。 JTAG（联合测试行动小组）、ISP（系统编程）和 Chip-off —— 与最新技术相反，它更多地依赖于取证技能，因此在此进行了简要介绍。

JTAG用于在制造后验证设计并测试印刷电路板。它涉及连接到标准测试端口以传输来自存储芯片的原始数据。ISP "是为了下载设备的完整内存而连接到 eMMC 或 eMCP 闪存芯片的一种做法"。Chip-off 是一种破坏性方法，该方法基于从系统板上卸下内存芯片，并且使用芯片读取器来提取存储数据。

最后，手动提取不需要复杂的工具，并且：

> " ... 只涉及滚动设备上的数据，并通过使用设备的键盘或触摸屏直接在手机上查看数据。然后将发现的信息以照相方式记录下来 ...... 在此级别上，无法恢复已删除的信息并获取所有数据。"

[image] *Cellebrite UFED Touch 2. Source: Privacy International*
[image] *Cellebrite UFED Touch 2 options. Source: Privacy International*

逻辑提取

"逻辑提取是关于提取逻辑存储对象，例如文件系统上的文件和目录。

使用设备制造商的应用程序编程接口来进行手机的逻辑提取，以使手

机中的内容与计算机同步。

许多取证工具都执行逻辑提取。它很容易执行，并且只恢复手机上的文件，而不恢复未分配空间中包含的数据。”

它是什么？

在三种提取类型中，逻辑被认为是最快的、最不侵入性的、但最受限制的。它会创建用户可访问文件的副本，例如电话簿、电话、消息、一些应用程序数据、以及您可能希望从
iTunes 或 Android 备份获得的其他数据。即 如果您手动检查设备上的每个屏幕，将会看到的东西。

MSAB 自称为 “移动设备取证技术的先驱”，它将其 XRY Logical 推销为 “我们为法证研究人员提供的入门级解决方案，以及我们许可证选项的起点”。

“ XRY Logical 使用户能够进行快速提取（iTunes 备份、Android备份、Android Agent），并且适合于 “抽检” 检查模式。”

[image] *MSAB's XRY Logical. Source: MSAB website* [image] *MSAB XRY Logical. Source: MSAB website* [image] *MSAB XRY Logical. Source: MSAB website* [image]

如果某些应用未备份到构成提取一部分的文件中，则逻辑提取可能会排除这些应用中的数据。要访问这些应用程序，您需要访问文件系统。

[image] *Magnet Forensics Webinar. Source: Magnet Forensics*

因此，您仅能获得可通过供应商的API获得的信息，手机会限制您可以访问的内容。但是，对于 Android 手机，可以通过将目标应用程序降级到允许adb备份的旧版本来获取应用程序数据。

据报道，此功能在较新版本的 Android 中被阻止。尽管 Cellebrite UFED 7.16 在APK降级方法上进行了更新，但它表示 “可以从运行6.0

及更高版本的 Android 设备上的40多个应用程序中访问文件系统数据”。

逻辑提取通常不包括数据的完整逐位副本，也不会恢复已删除的数据。但是，如果使用 SQLite 数据库（例如 Cellebrite 的 SQLite 向导）来存储数据，则可以恢复已删除的记录，包括短信、聊天记录和浏览历史记录。

它是如何工作的？

逻辑提取包括 “通过USB电缆、RJ-45电缆、红外或蓝牙将移动设备连接到取证硬件或取证工作站”。

连接电话后，取证工具 “启动命令并将其发送到设备，然后由设备处理器解释。” 取证工具与移动设备的操作系统进行通信。

> “… 从设备的内存中接收并发送回取证工作站。稍后，审查员可以检查数据。当前可用的大多数取证工具都在这一级别上工作。”

使用应用程序编程接口（API）是执行逻辑提取的一种方法。Cellebrite 是一家受政府机构欢迎的领先取证公司，他们说：“从技术角度来看，基于API的逻辑提取很容易实现，并且结果以可读格式提供。

Cellebrite 的 UFED Touch（带有UFED软件的硬件）和 UFED 4PC（安装在计算机上的软件）通过使用API与设备的操作系统进行通信来工作。

> “数据的逻辑提取大部分是通过设备供应商提供的指定*API*执行的。正如*API*允许商业第三方应用程序与设备*OS*进行通信一样， 它还支持取证声音数据 。

> 连接后，*UFED*将相关的供应商*API*加载到设备。然后，*UFED*进行只读*API*调用以从电话中请求数据。回复有效的*API*请求以提取指定的内容项，例如文本消息（*SMS*）、电话簿条目、图片等。”

使用 Cellebrite UFED Touch 2 在 iPhone 上进行逻辑提取的方式类似于 iTunes 或 iCloud 进行备份的方式，它在电话屏幕上显示提取数据的各种提示，例如“备份呼叫数据”（Y/N）

一些取证工具会将App或代理安装到设备上，以尝试提取其他数据。

> “最好的移动取证软件，例如：*UFED (Cellebrite), Oxygen Forensic, XRY (Microsystemation), Secure View (Susteen), MOBILedit Forensic* 都可以通过在设备上安装代理程序来从 *Android* 设备提取数据。”

MobileEdit Forensic 扫描连接的设备，如果检测到 Android 设备，则上传代理 Forensic Connector，并使用此代理从设备中提取数据。

即使解锁，也不保证所有设备都可以进行逻辑提取。例如Cellebrite的产品更新列出了支持的手机：

[image] *Cellebrite Product Update. Source: Cellebrite website*

利用漏洞

与所有形式的提取一样，有几个因素会影响是否可能。

首先是操作系统。如果是 Android，则已启用USB调试，从而启用了设备上的ADB服务器并且已接受RSA密钥（安全提示），已将个人计算机（“ PC”）和电话配对，于是可以执行逻辑提取。

如前所述，这通常是ADB备份，结合了将 Android APK 推送到设备并

使用可用命令来提取活动记录，如 SMS / MMS、呼叫日志和联系人。

Mikhaylov 指出，根据所使用的 Android 版本，激活USB调试模式需要采取不同的步骤。要启用USB调试，将需要密码。尽管某些运行Android的设备似乎是出厂时默认启用调试的（例如，隐私国际组织在2016–17年测试的 Innotab Max）。

USB调试模式是 Android 手机中的开发人员模式，它允许通过USB将新编程的应用程序复制到设备进行测试。它允许 Android 设备从计算机接收命令、文件等，并允许计算机从 Android 设备提取关键信息（例如日志文件）

启用USB调试会使设备暴露在外。 ADB Android Debug Bridge 是Google的 Android SDK 附带的命令行实用程序，它可以用计算机通过USB控制您的设备。

如果没有USB调试，除非使用漏洞，否则不太可能进行逻辑提取。

根据诸如电话类型、使用的漏洞、软件版本等因素，都有可能进行逻辑提取。

查看此问题的另一种方法是考虑用户数据是否存储在闪存中，如果存储，则是否受到保护并且需要root访问权限才能读取。

Magnet Forensics 的 Christopher Vance 描述了一个逻辑提取漏洞的示例，它只能针对文件系统的特定区域：

> “*/media/ directory* 可以容纳更多内容。它还可以包括文档、从*Web*浏览器下载的内容、*WhatsApp* 聊天备份、以及开发人员选择在此处存储的第三方应用程序数据。”

使用媒体传输协议（MTP）提取加密和损坏的 Samsung Galaxy S7

SM-G930V（无法输入密码或打开USB调试的情况下）是避免密码和授权的一种选择。

但是，虽然适用于某些 Android 手机，但三星v.6在将其插入计算机后已将默认连接类型更改为“仅充电”，因此必须启用MTP。Magnet AXIOM 具有“高级MTP旁路方法”：

> “ ... 为未收到 *SMR-OCT-2017* 或 *SMR-NOV-2017* 安全更新的三星设备获取设备上 / *media* / *partition* 的快速映像（修补程序的确切更新取决于设备型号）。iPhones 即使该设备未启用*MTP*或已被密码锁定，该选项也使我们能够提取一些数据进行分析。”

解锁 iPhones

虽然“ ... 解锁 iPhone 就可以获得逻辑提取”，但锁定的 iPhone 还是有问题的，因为有两种单独的状况要处理。

如果找不到标准的 iTunes 提供的驱动程序，并且默认恢复MTP模式，则激活与计算机的配对模式并允许 iTunes 备份；如果设备在进行提取的PC上具有有效的配对记录，则可以从锁定的 iPhone 获得逻辑提取。不幸的是，没有它就无法获得。

在较旧的iOS版本中，可以从已锁定的iPhone中仅获取MTP提取，但此问题已得到修补，新版本就不行了。

文件系统提取

从技术上讲，文件系统提取通常被视为一种逻辑提取。与所有形式的提取一样，文件系统提取的功能将取决于设备。

文件系统提取比逻辑提取能获得略多一些的数据，在文件系统提取

中，整个文件系统都能被提取出来。

> “它包含的信息比定义的逻辑提取要多得多，因此应被视为逻辑提取的进一步提升。文件系统包含设备用来填充应用程序、系统配置和用户配置以及用户存储区域的文件和文件夹。”

它包含用户无法通过设备界面直接访问的文件，并且需要专用工具来访问文件系统工件。它不会提取未分配的空间。

> 使用专有文件系统的功能手机可以收集并显示其文件系统，包括系统文件、用户数据库、媒体、用户文件、日志、用户设置等。 … 通过拥有实际的文件，您可以进行更详细的分析，应该认为它比“逻辑”所定义的价值更大。”

文件系统提取通常需要root，因为超级用户才有权对手机系统中任何位置的任何文件执行任何操作。

Cellebrite UFED 的 “高级逻辑提取” 结合了iOS和Android设备的逻辑和文件系统提取，是无法进行物理提取的替代方法。它们的解释是：

> 在使用*A5-A11*芯片（*iPhone 4s*和更高版本）的*iOS*设备上进行物理采集是不可能的。因此，高级逻辑提取方法是最好的支持，并且如果这些设备被解锁（即使它们没有越狱），也完全可以从这些设备中提取最多的数据。如果设备越狱，则可以提取其他数据。”

它是如何工作的？

文件系统提取很少被识别为一种独特的提取形式。而 Cellebrite 几乎独特地促进了UFED的文件系统提取，并且是少数引用该方法的公司：

> “使用 *UFED Physical Analyzer* 提取文件系统几乎与物理提取相同，因为它依赖于引导加载程序来访问设备的内存；但是，该软件不会仅提取设备文件系统而不获得包括未分配空间的逐位映像。 这种提取过程是专有的，而不是依赖于***Apple***的 ***API*** 。”

MSAB 没有特定的文件系统产品，仅是 XRY Logical 和 XRY Physical。Oxygen Forensics 是指将文件系统提取作为 “经典逻辑” 的一部分。

利用 Magnet 的提取工具，您可以选择提取过程，可以从所有iOS和Android设备进行 “快速提取”，也可以通过 “已root的 Android 设备的物理映像或越狱的iOS设备的文件系统逻辑映像” 进行全面提取。

> “如果设备已*root*，则可以创建物理转储。如果没有*root*，则会创建该设备的备份，并提取该设备的存储卡中的所有文件。”

但是，文件系统提取是无法物理提取iOS设备的替代方法。不幸的是，密码是必需的。

> “从*iOS 8*开始，即使在*32*位设备上，即便移除密码也是没有意义的。解密数据分区所需的加密密钥是根据用户输入（密码）和 *Secure Enclave* 的密钥动态计算得出的。没有正确的密码，*iPhone*将保持加密；根本没有办法解决。”

Secure Enclave 是 “基于硬件的密钥管理器，与主处理器隔离，可提供额外的安全性。” 结果是加密密钥受 Secure Enclave 保护，即使设备越狱也无法访问。

但是，“换句话说，必须知道密码，才能对从iPhone 5s开始的所有iPhone设备进行（有限的）物理采集。”如果您越狱了设备，则可以获得文件系统提取。为此，您需要使用密码启动和解锁设备。

> “换句话说，必须知道密码，才能对从 *iPhone 5s* 开始的所有 *iPhone* 设备进行（有限的）物理采集。*”*

> “ *Secure Enclave* 为*iOS*法证审查员带来了新挑战。现在，我们无法提取解密设备映像所需的加密密钥，因此物理提取无用。但是文件系统的提取可以。不幸的是，这要求将*iOS*设备越狱。”

与逻辑提取不同，一旦获得了文件系统，就需要对其进行解码。

解码过程将数据库文件中的原始数据转换为可识别的格式。通过API和备份提取的数据不需要解码，可以显示媒体文件，例如在设备上看到的图片和视频。但是，必须单独解码其他数据库文件（例如包含文本消息的文件）中的数据，以解析出这些消息。

UFED Physical Analyzer 会自动执行此解码过程，以人类可读格式以及原始数据存储在设备内存中的形式显示解码后的数据。” UFED Physical Analyzer 会自动执行此解码过程，以人类可读格式以及原始数据存储在设备内存中的形式显示解码后的数据。”

利用漏洞

Cellebrite 声称使用其内部实验室 “Cellebrite Advanced Services” 提取了iOS设备的完整文件系统，可以从32GB闪存中获取21GB。

Cellebrite 宣传其 “高级服务” 不是将重要的漏洞释放给 UFED，例如，这将为Apple提供修补漏洞的机会。而是没有公开披露的用于执行**iOS**设备的完整文件系统提取的漏洞。

[image]

这样做有三个主要好处。首先，可以从第三方应用程序获取数据，比如WhatsApp、Facebook Messenger、Telegram。除非执行完整文件系统提取，否则无法恢复数据。这些应用程序以及更多应用程序可以保存有助于您结案的关键信息。

即：完整文件系统提取可以获取 iTunes 备份中排除的第三方应用程序。它还可以识别目标设备的位置，显示系统日志和应用程序日志数据。

[image]

Cellebrite Advanced Services 的使用一直存在争议。去年6月，英国数字证据实验室 Sytech 的一名前雇员表示了对证据处理的担忧，其中包括“在没有监察的情况下将手机发送到国外进行解密”。

Magnet Forensics 还指出，它可以获取完整的文件系统。它与 GrayKey 合作提供了
“最先进的解决方案，可从iOS设备恢复数据，包括完整文件系统、解密的钥匙串和进程内存，而其他工具则仅限于 iTunes 备份。” 据说 GrayKey 可以解锁iOS设备并绕过USB受限模式。

Magnet Forensics 报告称，他们随后可以获取第三方应用程序数据，而不止 iTunes 备份、Apple Mail数据、Web缓存和应用程序缓存、操作系统数据、位置数据、钥匙串数据、和一些已删除的消息等方面：

> “ *GrayKey* 可以获取设备的完整文件系统映像，这意味着与我们的标准工件一起存在的临时文件或支持文件现在可供审查。
>
> 最好的示例是 *sms.db-wal* 文件，该文件与 *sms.db* 位于同一目录中。*sms.db* 允许检查者 恢复和解析 ***iMessage***、***SMS***消息和***MMS***消息 。

但是，由于该数据库利用了SQLite的“预写日志”功能，因此实际上将消息写入到 sms.db-wal 文件中，然后再提交到 sms.db。这可能会导致恢复可能已删除的消息时出现问题，具体取决于消息在删除之前在设备上的停留时间。

> 如果消息在发送/接收后立即删除，那么使用标准 *iTunes* 式提取来恢复这些消息的可能性要小得多。但

> 是，由于 *GrayKey* 允许我们提取完整的文件系统，因此我们现在可以访问此文件，并且 ***AXIOM*** 将尝试保留预写日志中留下的任何消息痕迹，包括可能删除的消息 。”

鉴于 iPhone 漏洞的价值，关于文件系统提取的信息很少。诸如 Android 之类的其他操作系统也没有太多信息，也许是因为仍然有可能执行作为首选的物理提取。

物理提取

物理提取可以获取 “服务数据、应用程序和用户数据”。可以从物理转储中恢复已删除的文件。

物理提取是物理存储/整个文件系统/设备内存的逐位副本，或作为十六进制转储。它通常需要特定的电缆连接，并且涉及将手机引导到自定义操作系统或重置。

物理提取通常会花费很长时间，因为它也会带来可用空间，但是可用空间可能包含已删除的信息，因此从警察的角度来看可能是值得的。

> “长期以来，物理提取一直是手机和嵌入式设备的理想取证方法。传统上，此方法包括对存储芯片的物理访问，以获得对基础闪存的原始读取。这种方法不仅可以访问数字数据，而且可以通过对物理存储进行快速分析，发现未使用的区域和块， 这其中可能包含已删除的数据并具有重要的取证价值 。”

它是所有提取中最全面、最具侵入性的，并且包含手机上所有未分配的空间，因此它可能包含已删除的文件。

Cellebrite 的物理提取功能可以访问已分配和未分配空间中的其他数据层，这些数据层构成了电话的物理内存。这些层包括与调查人员相

关的三组不同的内容：

- 无法通过API获得的“逻辑”内容（例如，手机上的通话记录）；
- 已删除的内容；
- 手机收集的内容无需任何用户操作（有时无需用户了解）。例如：Wi-Fi网络，GPS位置，网络历史记录，电子邮件标头以及图像和系统数据上的EXIF数据。”

[image]

它是如何工作的

十六进制转储，也称为物理提取，是通过将设备连接到取证工作站并将未签名的代码或引导加载程序推入手机，指示手机将内存转储到计算机来实现的。

> 由于生成的原始映像为二进制格式，因此需要技术专家进行分析。该过程... 为检查者提供了更多的数据，并允许从大多数设备上未分配的空间中恢复已删除的文件。”

MSAB 声明其 XRY Physical 产品通过绕过操作系统访问所有系统和已删除的数据。它们可以克服（某些）锁定设备上的安全性和加密挑战。

> “对移动设备数据的物理采集应该意味着与设备内部的数据存储进行直接通信，以采集存储在实际设备闪存中的数据。这些数据是闪存存储区域中的快照，可以通过专门的工具和方法来获取。”

> “ 在整个磁盘上启用加密功能后，除非检查员能够检索到设备的加密密钥，否则整个物理读取将无法使用

。

> *XRY Logical* 的 *XRY Physical* 插件可以让用户对一些 *Android* 设备进行密码旁路、板载存储芯片读取等高级移动取证任务。”

在 Android 手机上，此方法通常需要卸下电池关闭手机电源，而且充电线通常是专用的而不是使用标准的充电线。

Cellebrite 会全程指导必须进行哪些步骤，什么时候必须进行，包括开机时需要按住哪些按钮才能开启 FastBoot、Bootloader、Recovery、Factory Reset等，具体取决于目标设备。

设备进入 FastBoot 后，Cellebrite 的工作相当自动，它有时会提示你在手机屏幕上选择选项或重启手机。

物理提取, 我们做了一个 iPhone 4 的实验, 在iOS引导过程中使用的一个bug允许无符号代码执行 (其技术用于越狱旧的 iDevices) Cellebrite 然后运行了自己的操作系统，而不是iOS，以从手机中提取数据.

[image]

物理提取可能使用手机的救援模式或下载模式。”在这种模式下运行，手机在启动时，可以在RAM中插入一小段代码，称为引导加载程序”，引导加载程序会读取设备内存中的内容，并将其送回提取设备。Cellebrite 指出，”... 在设备启动的初始阶段，UFED 会将引导加载程序发送到设备上。

[image]

Cellebrite 的引导加载程序是针对每个单独的设备平台内部设计的，同时考虑了芯片组、外设、内存芯片接口和USB控制器的种类。

> *“UFED* 已经获得了数据解密后访问操作系统内部的权限。然后，它可以以解密形式提取原始的、块级的数据。再次通过利用 *Cellebrite* 发现的漏洞来实现。这些漏洞在被发现后很少会对公众开放。很多时候，

> ***Cellebrite*** 的安全研究实验室对漏洞及其带来的机会拥有独家了解 。

随着*iOS*和 *Android* 软件的发展，隐私保护、沙盒隔离机制和安全缓解措施的推进，这些知识只会变得更加值钱。*”*

iOS挑战

苹果的iOS系统为物理提取带来了最大的障碍。在 iPhone 4S 之前，你可以在 iPhone 上进行物理提取。但是自从 iPhone 4S 以及其他已经进入市场的设备，由于硬件加密的原因，要想进入到设备中是非常困难的，甚至是不可能的。虽然一些厂商的说法是 “可以”。

> “物理采集在恢复*iOS*设备上的数据方面具有最大的潜力；然而，这些设备上目前和不断发展的安全功能（安全引导链、存储加密和密码）可能会阻碍数据在取证过程中的可访问性。
>
> 研究人员和商业取证工具供应商正在不断尝试新的技术来绕过安全功能，在*iOS*设备上进行物理提取，但对于最新的机型来说，唯一可用的选择就是越狱，即使是这样也无法帮助你用 ***Secure Enclave*** 对设备进行物理提取 ……*”*

Elcomsoft iOS Forensic Toolkit 5.0表示，它可以实现iOS 12的物理提取。这听起来和上面介绍的Cellebrite的全文件系统提取类似。它可以提取文件系统的内容，并解密**iOS**密钥链中存储的密码和验证凭证。在 “没有越狱 “支持的设备上都可以实现。

> *“Elcomsoft iOS Forensic Toolkit* 支持从越狱和非越狱的*64*位设备中提取和解密数据的所有可能选项，包括上一代苹果硬件和软件。
>
> 在没有越狱的情况下，可以通过*iOS*系统备份、提取

共享的*App*数据和媒体文件，进行逻辑提取。

在某些情况下， 如果 ***iPhone*** 被锁定，甚至也可以进行逻辑提取 。如果能越狱，就可以对*64*位 *iPhone* 的文件系统进行镜像，提取受保护的应用数据和工作数据集。”

“ 物理采集与所有其他采集方式相比具有众多优势，可以访问文件系统中受保护的部分，并提取不与 ***iCloud*** 同步或不包含在本地备份中的数据。

特别是，物理提取是唯一一种针对最高保护级别的密钥链项目的解密方法。文件系统提取可以获得对应用沙盒和所有系统区域的完全访问权限， 提取私密聊天记录，恢复已删除的邮件，下载电子邮件、聊天记录和双因素身份认证应用中的秘密、系统日志和详细的位置数据等，都是文件系统提取的独家功能。 ”

针对 iOS 11 设备的 Elcomsoft iOS Forensics Toolkit 使用经典越狱。

“取证专家们使用越狱的原因与热心用户相比有很大不同。安全漏洞正是他们想要暴露设备的文件系统、规避iOS沙盒保护和访问受保护的数据的途径。越狱可以从设备中提取最大的数据集。在越狱过程中，iOS的许多软件限制都是通过软件漏洞来消除的。

除了沙盒之外（包括对话历史记录和下载的邮件），还可以提取和解密钥匙链，这是一个广泛存储在线密码、认证令牌和加密密钥的系统。与从受密码保护的本地备份中获得的钥匙链项目不同，越狱设备的物理提取可访问具有最高保护等级的钥匙串项目。”

Android – Using vulnerabilities：紧急下载模式

“这似乎不寻常，但可以在不进行*root*的情况下对安卓设备进行物理转储，不需要 *JTAG* 和 *Chip-off* 方

法。”

紧急下载（EDL）模式是一个被用来进行物理提取的漏洞。它适用于部分但不是所有搭载高通芯片组的设备。EDL是高通公司用于手机诊断和修复的救援模式，它通过各种触发器或当设备无法启动时暴露出来。它“设计用于允许低级别访问芯片组以进行设备分析、维修或重新设计。”

Cellebrite 公司有多种准备好的“编程器”，这些“编程器“是“包含原始闪存读写功能的软件片段”。可以通过设备验证的厂商签名进行数字签名，所以要让EDL接受和验证一个编程器，它必须与硬件和签名要求相匹配。

当 Cellebrite 的UFED启动 EDL 提取流时，它将自动尝试将其现有编程器与硬件和签名要求进行匹配。如果有匹配，那么它将拥有闪存的读取权限。如果对某款手机没有签名需求，那么它就会匹配硬件。据 Cellebrite 称，**UFED**有一个专有的漏洞利用，可以绕过多个芯片组的签名要求。

将设备置入EDL模式的方式因手机而异，从 Cellebrite 的UFED等各种可以支持的技术到需要取证技巧的侵入性技术，不一而足。如果 Cellebrite 支持 EDL，UFED 可以指导你做什么，比如说，按住VOL向上和向下。

Cellebrite 的 UFED 有解密和非解密 EDL 提取选项。如果设备被加密，这两种方案都可以在模式或密码锁定的设备上工作。加密设备的解密提取将需要设备启动，这样UFED就可以应用解密引导加载程序，而非解密EDL提取则不需要。

[image]

对于这两个选项，在使用UFED时，用户将能够选择将设备置于DFU（诊断模式）FTM（出厂测试模式）。这两种模式都使用EDL方法。

Cellebrite 还提高了使用“智能” ADB的能力：

> “凭借这一突破性的功能，*Cellebrite* 可以在启用*ADB*的情况下恢复对许多启用了全盘加密的新设备的物理提取访问权限。该方法需要安卓6及以上版本，并对许多厂商有广泛的通用覆盖。”

Oxygen Forensic Detective 指出，使用EDL模式“可以使研究人员在电话成功进入EDL模式后，在400多种独特设备上利用这种非侵入式物理提取技术和锁屏旁路。”

[image]

分析：对提取的数据进行分析

有许多具有令人印象深刻的分析功能的工具，可帮助警察处理提取出来的数据。

> “有很多工具可以对运行 *Android* 操作系统的移动设备进行物理转储和备份分析。这些工具包括在所有最好的移动取证工具中，如*UFED*物理分析器（*Cellebrite*）、*Oxygen Forensics*（*Oxygen Forensics*，*Inc*）、*XRY*（*MSAB*）、*MOBILedit Forensic Express*（*COMPELSON Labs*）和*Secure View*（*Susteen*）等。”

> “使用第三方工具进行检查和分析，一般是将设备的内存转储导入移动取证工具中，由移动取证工具自动调取结果。”

Cellebrite 的物理分析器是一款用户友好型软件，可以组织不同文件类型的数据，从 XML、CSV、TXT 到 CDR、媒体和文本等。它可以将来自不同设备的数据集汇集在一起，对数字媒体进行识别和分类。可以显示提取的所有信息。它还具有相当大的数据挖掘和可视化功能。

关系分析是用来分析电话、邮件文本和位置数据，通过不同类型的数据发现个人之间的关系。正如 Peter Sommer 教授在向英国议会作证时指出的那样：

> “它还利用数据可视化/联系分析技术来展示电话号码之间、*IP*地址之间的联系频率、金融交易和事件年表等。

英国警方正在试用 Cellebrite 的机器学习工具，以解释图像、匹配面孔并分析目标人的交流方式。

Cellebrite 指出：

> “… 数据可与其他关键信息来源一起提取，如电子邮件和社交媒体账户的在线活动等。
>
> 然后利用人工智能和机器学习对这些来源进行过滤、比较和分析，以产生可操作的洞察力，如地点定位等。
>
> 提取的数据可以与网站或社交媒体账户等公共来源的数据相结合，以找到关键信息并进行比较 。
>
> 警察可以利用这些综合数据建立目标人的详细档案。这些数据还可以建立目标事件的时间线，帮助警察确定发生了什么，并为起诉汇编正确的证据。”

Magnet AXIOM 还利用机器学习：

> “机器学习通过 *Magnet.AI*，提供……….一种经过“训练“的预测仪器，可以识别属于………类别的信息。”

> “随着 *AXIOM 2.0* 的推出，*Magnet.AI* 模块现在可以识别可能包含儿童性侵、裸体、武器和毒品等描写的图片。 我们还扩展了文本分类模型，还能检测出潜在的性暗示对话 。”

2017年8月，Cellebrite 为其分析平台推出了所谓的 “先进机器学习技术”，可用于分析从云端提取的数据，其中包括人脸识别和匹配。

从2019年7月起，Oxygen Forensic Detective 内置的 Oxygen Forensic JetEngine 模块，利用自身技术对人脸进行分类。

不仅提供提取数据内的人脸分类和匹配，人脸分析还包括性别、种族和情绪识别。

Oxygen 的首席运营官 Lee Reiber 表示，该工具可以 “在证据库中搜索特定的人脸，或者将同一人的各种图像聚在一起。他们还可以根据种族或年龄组，以及 “喜 “和 “怒 “等情绪来过滤人脸。”

[image]

结论

随着移动电话提取的使用越来越多，无论是警察还是边境安检，这些设备的数据将被用于对个人提出质疑，无论是刑事、民事还是移民诉讼和程序。

虽然移动取证是一个快速变化的领域，但本文是一个尝试，可以帮您看到当那些使用强大的提取工具从设备中寻找数据的家伙正在干什么。

移动取证的使用提出了与作为证据形式的提取数据的可靠性有关的复杂问题，特别是，如果是由依赖简单的按钮技术而不是数字取证分析专业不熟练的人使用时，更是如此。

正义的实现取决于证据和信任的完整性和准确性。我们希望，在开始消除该领域的某些复杂性时，我们可以为有关该主题的辩论提供足够的信息。

[image]
[image]

间谍机构使用的开源情报监视方法

[image] 关键词	反监视 反追踪 开源情报
[image] 关联	🔍开源情报
[image] 创建时间	2020年10月20日
[image] **Description**	技术直觉

从专业级别讲清开源情报的基本操作。其中关联的所有文章都很重要；穿插的所有书籍均免费下载

- Table of Contents

开源情报的来源可以包括：
为什么开源情报对于调查很有价值？
开源情报流程的各个阶段
开源情报侦察可进一步细分为以下**5**个子阶段：
对开源情报工具的研究
1、搜索引擎
2、图像
3、社交网络
案例管理和方法论
案例管理
下面是最流行的基本开源情报技术流程：
最后强调：

[image]

以下段落摘自CIA官方网站。

> 总统和政策制定者依靠中央情报局的见识来为自己的外交政策决策提供依据。中央情报局官员在制定评估时使用了多种渠道 ……本文将重点考虑开源情报。

信息不一定必须是秘密的才能有价值。

无论是在浏览的博客中、在观看的广播中、还是在阅读的专业期刊中，都有无穷无尽的信息来帮助我们了解世界。

情报社区通常将此信息称为开源情报。

开源情报在以其相对较低的成本为情报界提供整体见解和背景方面发挥着至关重要的作用。

[image] 图中这本书在这里下载：https://www.patreon.com/posts/kai-yuan-qing-de-38190146

开源情报的来源可以包括：

- 互联网
- 传统大众媒体（例如电视、广播、报纸、杂志）
- 专业期刊、会议记录和智囊团研究
- 各种照片
- 地理空间信息（例如 地图和商业图像产品）
- 等等……

[image] 上图中这本书在这里下载：https://www.patreon.com/posts/tu-xiang-qing-38190530

CIA 通过其对DNI开源中心（OSC）的管理，负责收集、生产和推广开源情报。OSC 成立于**2005**年11月1日，是根据大规杀伤性武器（Robb-Silberman ）委员会的建议而成立的，其职责是承担整个情报社区的独特责任。

民间社会组织及其全球合作伙伴网络拥有制作高质量开源情报所需的技能、工具和渠道。这些能力包括**80**多种语言的翻译；来源、趋势和媒体分析；专门的视频和地理空间情报分析；以及罕见的文化和特定主题的专门知识等。

对于OSC主管 Douglas Naquin 来说，牢固的合作关系至关重要。

> “鉴于我们可以通过公开信息解决的问题种类繁多，范围广泛，我认为我们有责任在政府内外各组织之间进行合作，最有效地利用现有的专门知识和能力。我们 OSC 的工作重点是比较优势：如果我们发现一个组织或公司能把某件事做得特别好—— 例如翻译—— 我们将尽可能地利用这一优势，使我们能够把资源集中在我们最擅长的方面。”

【注】上面这段话用一个词概括就是：收编。准确说是 “公私情报伙伴关系”。

开源情报 一直是 “全源” 情报分析的重要组成部分，尤其是，信息技术的不断发展使更多的人发出了声音，从而更有可能解决新的情报问题。（【注】“更多人发出声音” 指的是人们在社交媒体上说的太多了）

[image] 上图中的内容在这里看到：https://www.patreon.com/posts/dui-kang-xing-si-38187798

“例如，公开的消息来源可以告诉我们海外各种团体对总统演讲的反应”，Naquin 说。“我们不必满足于 ‘官方’ 的观点，而是可以评估各种群体的看法，以及跟踪一段时间内的趋势。”

“开源是指 ‘免费’ 或公开的情报来源，但并不意味着它很容易得到”，

Naquin 补充道。为了过滤、理解和分析24/7进入OSC的大量材料，开源情报官员必须精通外语，对文化的细微差别很敏感，是各自领域的专家，无论是视频、地理空间工具、媒体分析还是图书馆学方面。

“如果一个政府改变了对美国的立场，一个对语言理解透彻、对文化熟悉的分析人员可能不仅能够预测这种变化，而且能告诉我们原因。” Naquin 说。“能够将外语技能、文化知识和先进的搜索技术结合起来的人并不多见。”

[image]

对这段话的具体解释，推荐这份报告 https://iyouport.substack.com/p/bb3?utm_source=publication-search。

简单说，全世界所有人的一切信息都在被这样收集和分析，大多数国家都在做这样的事，而不仅仅是美国和中国（虽然中美在这方面有最显著的优势。因为绝大多数互联网服务不是中国的就是美国的）

政策制定者和其他政府官员也依靠这些专业知识来了解他们计划访问的国家的概况。

“不仅仅是指南信息，而是有助于让他们的访问富有成效的细节。如果知道去哪里找的话，在开源情报中能找到的东西是令人惊讶的。”

OSC 将其收集和处理的大部分信息提供给情报界和整个政府。除了向所有来源的对应方提供这种“原始”数据外，OSC的分析人员还从公开来源中发现并为他人标明新的见解或趋势。

一个有经验的情报分析师会注意到外国政府和组织官方信息中的语气、选词和语法的变化。与过去的声明进行比较，可以深入了解外国行为者如何看待一个事件或问题。这种分析还可以帮助确定他们的“热点“或“红线”。

[image]

这也是为什么我们强调：政治评论应该以情报分析的思考方式而不仅

仅是观点来呈现。

[image] 上图中这本书在这里下载：https://www.patreon.com/posts/cong-jian-die-de-38188158 [image] 上图中这本书在这里下载：https://www.patreon.com/posts/38138056

与所有情报学科一样，开源情报也有其挑战。庞大的数量令人望而生畏，要想把麦子从谷子中分离出来，需要很多技巧、知识和对尖端信息技术的娴熟。

它还需要协同努力，与合作伙伴进行协调，以避免重复、并以最佳方式利用资源，但开源情报在效力和效率方面的回报是很高的。

Naquin说，“我们工作在两个最具活力的行业的交汇处：媒体和信息技术。这就像坐着皮划艇在两条河流的分叉处顺流而下，这一路会很有挑战，但如果你有技术，它就会很精彩。”

互联网已经彻底改变了开源环境。 Naquin 预计这种趋势将持续下去。

他说，“今天投资于开源情报的组织，就好比一个人在谷歌成立的第一年投资于谷歌。开源情报一直是情报工作中不可或缺的组成部分，但我相信五年后，其价值只会增加。一个对开源情报的价值和潜力有认识的组织在未来将是最有效的组织”。

[image]

为什么开源情报对于调查很有价值？

开源情报之所以有价值，是因为相比诸如 HUMINT、SIGINT、MASINT、GEOINT 等具有更多的技术需求的情报学科来说，开源情报具有更少的严格性和开发过程、以及时间表，此外，开源情报收集了各种各样的宝贵意见，因为它涵盖了各种各样的资料来源。

开源情报为理解机密材料提供了基础。尽管情报社区产生了大量的机密材料，但在任何一个主题上产生的机密信息数量都可能非常有限，如果仅从机密来源的角度来看，可能会脱离背景。

[image]

开源情报和透明度革命应该相辅相成、互相协助，而不是像今天这样互相排斥。并且已经有成功的融合案例，见 https://iyouport.substack.com/p/lr--e6e?utm_source=publication-search ，这篇文章中详细解释了这个问题。

开源信息可以填补空白并创建关系联系，使分析人员可以更好地理解零散的情报、可能的攻击手段以及潜在的目标。

开源材料可以保护资源和方法。有时，可以在开源报告的基础上解释实际上被告知敏感的机密信息的情报判断。当政策制定者需要解释政策决定或与外国官员沟通而又不至于损害机密消息来源时，这点就会很有用。

只有开源情报才能存储历史。一个强大的开源情报调查实际上可以收集数据来监测全世界上的文化、以及它们是如何随着时间变化的。使用闭源收集方法提供的快照要想做到这点，即使不是不可能，也是很困难的。

先进的数据分析改变了间谍机构利用数据的方式。另一方面，这些间谍机构正在被不断增长的数据洪峰所淹没。虽然数据驱动的警务正在兴起，但执法人员尚未意识到态势感知的全部好处 —— 如何帮助他们从噪音中区分信号。

开源情报流程的各个阶段

开源情报通常在黑客入侵的侦察阶段进行，从这一阶段收集到的相关信息会被带到网络枚举阶段。

由于网络上有大量的信息可供筛选，攻击者必须有一个清晰明确的搜索框架，以及一系列开源情报收集工具来促进这项任务，并协助处理数据；否则就有可能迷失在互联网上铺天盖地的信息海洋中。

开源情报侦察可进一步细分为以下5个子阶段：

1、源头识别：作为起点，在这一初始阶段，执行者需要识别可能收集到信息的潜在来源。在整个过程中，消息来源要以详细的笔记形式记录下来，以便以后在必要时再来查阅。

2、数据采集：在这个阶段，执行者从选定的来源和整个阶段发现的所有其他来源收集和采集信息。

3、数据处理和整合：在这个阶段，攻击者通过搜索可能有助于情报产品的信息，对收获的信息进行处理，以获得可操作的情报。

4、数据分析：在这个阶段，执行者利用各种开源情报分析工具对处理后的信息进行具体分析。

5、成果交付：在最后阶段，完成开源情报分析，并将分析结果提交/报告给红队或其他需求方。

下面将介绍在开源情报调查和分析中要使用的一些工具，以及如何有效地使用这些工具。

有大量的开源情报工具可供使用，其中一些是免费的，而另一些则可能要花不少钱。

执行开源情报就是把您能够推断出的关于某个人或实体的零星信息，通过情报分析工具执行它们，看看还能发现什么。

对开源情报工具的研究

以下是一套选定的工具，说明了开源情报工具之间的不同。

这些解决方案代表了不同类型的用例，为可用的开源情报解决方案的规模提供了更广阔的视野。

开源情报解决方案的范围通常非常广泛 —— 这些工具可能被设计成只关注单一的查询，而更强大的开源情报解决方案则有能力进行更大规模的查询。

许多规模较大的开源情报工具都是为政府和巨头公司定制和设计的，预算巨大，自然只有这些有钱有势的家伙才能使用。

这些工具具有强大的自动化流程、人工智能和先进的过滤技术。无疑，公民调查人员无法接触到这样的工具。然而，公众通常可以访问的工具和资源的数量也是尤其显著的，可以进行强大的搜索。

1、搜索引擎

根据调查背景，您可能想在调查期间使用不同的搜索引擎。Google 和 Bing 用于欧洲或北美的相关调查主题，百度用于亚洲的相关调查主题，Yandex 用于俄罗斯和东欧的相关调查主题。

当然，第一个调查工具就是搜索运算符。您可以在下面找到谷歌的这些搜索运算符的基本列表。

[image]

延伸：https://iyouport.substack.com/p/735?utm_source=publication-search

延伸：https://iyouport.substack.com/p/googledorking-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/d91?utm_source=publication-search

其实您记住一些基本常识就可以，比如，在搜索下面这些内容时，必需用引号将它们扩起来：

- 电子邮件地址
- 电话号码
- 用户名
- PIN码

[image]

延伸：https://iyouport.substack.com/p/305?utm_source=publication-search

您还可以使用布尔逻辑运算符进行组合查询：AND，OR，＋和-。

- filetype: 允许搜索特定的文件扩展名
- site: 将在特定网站上过滤
- intitle:和 inurl: 会过滤特定标题或 url
- link:: 查找指向特定域名或URL 的网页（于2017年弃用，但仍然可以部分使用）

还有以下这些例子：

- NAME ＋ CV ＋ filetype:pdf 找到目标人的简历
- DOMAIN—site:DOMAIN 找到网站的子域
- site:example.com/folder: 如果您知道某个站点的基本架构，则可以结合使用，例如：site：amazon.com/China
- site:sub.example.com: 帮助深入研究特定的子域。例如 site:local.amazon.com
- site:example.com inurl:abc: 找到子域。使用 “inurl:” 比直接将子域放入主查询要灵活得多。例如，site:amazon.com inur:local
- site:example.com inurl:https: 这种组合有助于查找 Google 编入索引的所有安全页面。例如，site:amazon.com

2、图像

对于图像，您需要了解两件事：如何查找图像上包含的任何其他信息、以及如何查找相似的图像。

首先就是从元数据入手。它通常包含创建日期、使用的相机、有时是GPS数据等丰富且危险的信息。

ExifTool 是很好的选择，但 Exif Viewer 扩展也非常方便（适用于 Chrome 和 Firefox）。此外，您还可以使用这个惊人的照片取证网站，有许多有趣的功能。其他的替代方案包括 exif.regex.info 和 Foto Forensics。

[image]

在本站“工具-Tools ”专题中搜索“元数据”，以找到很多相关工具。

要找到相似的图片，您可以使用 Google Images、Bing Images、Yandex Images 或 TinyEye。TinyEye 有一个有用的API，Bing 有一个非常有用的功能，可以让你搜索图像的特定部分。为了得到更好的结果，删除图片的背景可能会有帮助，于是 remove.bg 可以帮助您做到。

不同的图像工具有不同的特点，根据您的具体调查需求来选择，于是您最好能熟知它们各自的特征。

并没有简单的方法来分析图像的内容并找到它的拍摄位置。您必须在图像中寻找特定的线索，然后在网上进行研究，并与原始图像进行比较。

3、社交网络

社交媒体情报是开源情报的重头戏，于是从社交网络上挖掘情报的工具特别丰富。但是这些工具的效果在很大程度上取决于具体平台。

[image]

延伸 - 一些基本方法：https://iyouport.substack.com/p/6f5?utm_source=publication-search

比如 Tinfoleak.com，可以在其中获取有关任何 Twitter 用户的详细信息。它是完全基于Web的，不需要用户进行任何安装。

要想通过 Tinfoleak 从 Twitter 上获取用户相关数据，只需要提供目标用户的 Twitter 用户名，只能是公开用户。

作为查询的结果，Tinfoleak 会提供一份关于目标用户的详细报告。该报告提供了用户的基本信息（如姓名、照片、位置、关注者等），以及 Twitter 用户使用的设备、操作系统、应用程序和社交网络的信息，Twitter 用户访问过的地点和地理位置坐标，允许下载 Twitter

用户的所有图片，还显示了 目标 Twitter 用户使用的所有标签和话题（含日期和时间），以及目标用户在其推文中提到过谁。

Tinfoleak 还利用推文和图片中的地理信息定位用户发推的地方。

工具总是那么令人兴奋，但是，必须强调：工具并不重要，重要的是您用工具做什么。如果您不知道自己在做什么，工具并不会帮助你，它们只会给你一长串你无法理解或评估的数据。

您需要的是，测试工具，阅读它们的代码，创建自己的工具等等，但要确保您了解它们的工作方式。最好的工具箱是你足够了解、喜欢并能够熟练掌握的工具。理论上这并没有普适的列表，对于政府间谍来说也一样。

案例管理和方法论

情报收集计划 ICP 是大多数现代武装部队和情报部门使用的系统过程，通过分配所有可用资源的任务来满足情报要求，以在规定的时限内收集和提供所有相关信息。制定收集计划是情报周期的一部分。

尽管 ICP 没有规定的格式，但它必须使用所有可用的收集功能来满足决策者的优先级要求。它必须精确而简明，但也要足够灵活，以应对变化的发生。

切勿因觉得自己国家的间谍机构无法获得哪里的信息，就认为此处“安全”，因为没人能说清楚全世界究竟有多少情报共享 —— 直到它们被揭露。比如https://web.archive.org/web/20200916144341/https://www.iyouport.org/%E6%B2%A1%E6%9C%89%E7%BE%8E%E5%9B%BD%E7%9A%84%E4%BA%94%E7%9C%BC%E8%81%94%E7%9B%9F%EF%BC%8C%E8%A2%AB%E4%BF%9D%E5%AF%86%E4%BA%86%E8%BF%9150%E5%B9%B4%EF%BC%8C%E4%BB%8A%E5%A4%A9%E4%BE%9D%E7%84%B6%E6%B4%BB/

案例管理

组织是效率的关键，对于减少错误和混乱、节省时间和金钱、以及提高结果的整体质量至关重要。

如果您买不起花哨的案例管理软件，如 i-sight / Maltego ...... 也不用担心，Zotero 已经基本覆盖了主要功能。

Zotero 可帮助您以任何方式组织您的研究资料。您可以将项目分类到集合中，并用关键字标记它们；或创建保存的搜索，这些搜索会在您调查工作中自动填充相关材料。

尽管有很多开源情报技术和机制，但并不是所有的技术和机制都能为您的调查目标服务。

所以，首先您将不得不问自己至少以下这些问题：

- 我在找什么？
- 我的主要研究目的是什么？
- 我的追踪调查目标是谁或什么？
- 我该如何进行研究？

请找到有关这些问题的尽可能准确的答案。这是进行任何开源情报调查的前提。你必须确定哪些来源是好的，哪些来源与你的研究无关。

下面是最流行的基本开源情报技术流程：

- 收集员工的全名、职务和他们使用的软件；

- 查看和监控来自 Google（尤其是使用 Google Dorks）、Bing、Yahoo 等网站的搜索引擎信息；

- 监视个人和公司博客，以及在数字论坛上查看目标用户活动（跨站追踪）；

- 标识目标用户或公司使用的所有社交网络；

- 查看社交网络（如 Facebook，Twitter，抖音、LinkedIn 等等）上所有可用的内容； [image]自我人肉

- 使用 Pipl 等人员数据收集工具，该工具将帮助您在一个地方揭示有关目标个人的大量信息；更多 “搜人”引擎在这里、这里、和这里找到；

- 从Google访问旧的缓存数据 —— 通常会显示有趣的信息， https://web.archive.org/web/20201031192212/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E5%BF%AB%E9%80%9F%E6%89%BE%E5%88%B0%E4%BD%A0%E6%83%B3%E8%A6%81%E7%9A%84%E4%B8%9C%E8%A5%BF%EF%BC%9A%E8%BF%BD%E8%B8%AA%E6%95%B0%E5%AD%97%E8%AF%81%E6%8D%AE%E7%9A%84%E5%B0%8F%E6%8A%80/；

- 识别手机号码、以及来自社交网络或 Google 搜索结果的邮件地址；

- 在常见的社交照片共享网站（例如 Flickr、Google相册等）搜索有关目标人的一切照片和视频；

- 使用Google地图和其他开放式卫星图像资源检索能够暴露目标用户地理位置的图像；

- 使用 GeoCreepy 之类的工具来跟踪地理位置信息，以清楚地了解用户的当前位置；

- 使用自动化的开源情报工具检索信息，例如 Spiderfoot 或 us；

- 使用 OSINT Browser 之类的资源；

- 使用 SecurityTrails 工具包探索DNS以及域、子域和IP地址；

- 针对目标服务器基础结构运行端口扫描程序以查找正在运行的服务；

- 使用 Shodan 搜索目标的所有联网设备。

您会发现的一些最流行的技术。然而，在做完开源情报研究之后，您会有很多数据需要分析。这时，您就必须完善刚才的调查结果，并详细搜索所需要的所有真正必要的东西，放弃其余的东西。

您到处都能找到的经典开源情报方法论是僵硬的：

1. 定义要求：您在寻找什么？

1. 检索数据

1. 分析收集的信息

1. 数据透视和报告：要么通过透视刚刚收集到的数据来定义新需求，要么结束调查并编写报告

这个方法论很直观，但可能帮不上什么忙，但您还是要照顾它，花时间做一个循环迭代。很多时候，在调查过程中，您会迷失在收集到的大量数据中，很难有一个对调查方向的看法。在这种情况下就休息一

下，回到上述第三步和第四步是很有帮助的：分析和总结你所发现的所有东西，列出可以帮助你校准目标的东西，并定义新的（或更精确的）仍然需要回答的问题。

[image]

保留证据很重要：信息在网上消失的速度非常快。想象一下，您手滑在推特上点了一个赞，于是被调查对象开始怀疑了，突然间，您想要追踪的所有目标人的社交媒体账号和网站在一天之内全部消失……

所以要保留证据：截图、档案、网络档案、或者其他任何对你有用的东西。

[image]

延伸 - 如果真的手慢了怎么办？还可以从这里的方法补救：https://iyouport.substack.com/p/305?utm_source=publication-search

在取证中，时间线和对同一时间内发生的事件进行定位是一个关键。它在开源情报中绝对没有那么重要，但仍然是一个非常有趣的工具可以帮助组织您收集到的数据。

比如，该网站是什么时候创建的？目标的 Facebook 账户是什么时候创建的？最后一篇博客文章是什么时候完成的？……把这些都放在一个表格里，往往能让您很好地看到您要找的东西。

描述工作流程的流程图很重要，以根据数据类型（如电子邮件）搜索更多信息。

随时记得安全！是您在调查目标，而不能让目标意识到这点，反过来调查您。所以，在隐身层面谁能做到更好，谁就能取得胜利。

最后强调：

1. 本文取自专业政府间谍对开源情报的使用 —— 包括监视社交媒体情报以扼杀所有反抗；

1. 因此，您完全可以用这套方法来调查您自己和您的组织，抢在坏人前面堵住您发现的任何泄漏；

1. 本文中关联的所有书籍均免费下载，如果您希望深度研究该领域，这些书籍都很有用。请记得，下载后个人阅读没有任何问题，但您不能出售它们以盈利。

[image]
[image]

一些简单的措施以防止您的汽车被骇客控制

[image] 关键词	汽车 物联网 网络攻击
[image] 关联	[image]你家冰箱如何作为呈堂证供？ ；[image] “智能城市”究竟是个什么鬼
[image] 创建时间	2020年12月2日
[image] **Description**	技术直觉

当您选购汽车的时候，除了看颜值和性能之外，还必须注意其他东西……

- Table of Contents

  您的汽车可以被黑客入侵吗？
  您能保护自己吗？
  密钥卡（就是汽车钥匙）
  移除**OBD II**加密狗
  防止网络钓鱼
  不要惊慌

[image]

汽车黑客正在成为一个严重问题。

随着汽车与互联网的连接越来越多，每款新车型都会有新的连接，您理所当然地应该考虑到：至少，如今正在出现一种新型的劫车行为。

目前这种情况还相对罕见，但实际上已经发生了。虽然目前的方法还不能关闭汽车发动机，但无需钥匙进入您的汽车的黑客方式已经成为现实。这会威胁到您的财产。

[image]

延伸：https://iyouport.substack.com/p/11-f2e?utm_source=publication-search

延伸：https://medium.com/@iyouport/%E5%B0%8F%E5%BF%83%E4%BD%A0%E7%9A%84%E6%B1%BD%E8%BD%A6%E5%8F%98%E6%88%90%E9%97%B4%E8%B0%8D-%E5%A6%82%E4%BD%95%E4%BB%8E%E8%81%94%E7%BD%91%E6%B1%BD%E8%BD%A6%E4%B8%AD%E5%88%A0%E9%99%A4%E4%B8%AA%E4%BA%BA%E9%9A%90%E7%A7%81%E6%95%B0%E6%8D%AE-604be580e962

无钥匙劫车并不是联网汽车的唯一问题，也不是其唯一的弱点。从好的方面来说，今天，您也许还不需要担心自己的人身安全；但明天或后天可能就需要担心了。尤其是随着黑客技术越来越复杂的发展趋势。

[image]

您的汽车可以被黑客入侵吗？

现代的 “智能” 汽车或网联汽车当然最容易受到汽车黑客的攻击。但老款汽车也是脆弱的，虽然程度不同。Andy Greenberg 决定成为汽车黑客实验的小白鼠。坐在后座上的两位黑客在 Andy 驾驶的情况下操纵了这辆汽车。

黑客们成功远程控制了这辆福特Escape。这些家伙从美国国防高级研究计划局（DARPA）获得的资金，用于寻找汽车的安全问题。看来这笔钱花得很明智。

他们成功地玩转了对仪表盘和其他小系统的控制，比如燃油表。他们

还成功地阻止了汽车的刹车工作，并操纵了转向系统。这已经足够让人惊心动魄了。

在这段视频中，黑客是直接坐在汽车上的，但他们也成功地做到了远程控制。

您能保护自己吗？

如果您拥有这些精美的、已联网的，启用了应用程序的现代车辆之一，您也并非只能束手无策。

Mercury Insurance 保险集团制作了一个简易的指南，帮助您找出您的车辆的弱点。他们甚至提供了帮助您保护汽车的信息。

他们的数据库里有大量的汽车品牌和车型，并为您提供了一个漏洞检查的分数，满分为6分，它的分数基于一系列的黑客入口点，包括无线胎压、蓝牙、导航、密钥卡、车载WiFi和多媒体系统。都是汽车黑客的潜在切入点。

您可能认为这只是新车的问题，但是，老车也会被 “黑”。比如研究人员检查了一辆2003年的老款大众高尔夫，发现它的密钥卡系统存在黑客漏洞。相当吓人。

虽然黑客对汽车的远程整体控制能力有限，但是，他们的确能够进入汽车，甚至启动发动机！不妨检查一下自己的车。

密钥卡（就是汽车钥匙）

到目前为止，最常见的问题是通过汽车密钥卡未经授权进入。专家建议通过将密钥卡放在冰箱或微波炉里来避免这点 —— 基本上是像法拉第笼一样的东西，就像您保护自己的手机避免远程控制那样；或者用铝箔纸包裹，再或者您可以直接买一个RFID 信号阻挡钥匙扣保护器。后者是最安全的，老实说也是一种不太奇怪的方法，此外如果您

在加热食物前忘了把密钥卡从微波炉里拿出来 ...就麻烦了。

移除OBD II加密狗

车载诊断系统（OBD）II加密狗是一些保险公司提供的监测您驾驶习惯的设备。对于被认为 “更安全” 的司机来说，可以收获更低的保险费。

它们通过转向柱下方的一个端口连接到您的车子。这显然为潜在的黑客提供了一个非常诱人的 “后门” 入口。所以，当它不被使用时，您需要拔掉它的插头或把它完全移除。

防止网络钓鱼

现在有些车子已经可以用手机启动。但是您必须想到：如果您能用手机启动，那么其他人也可以做到！挪威的一些研究人员演示了这种技术 —— 他们不仅可以窃取您的所有的信息，还能通过公共WiFi用手机把你的车开走。

网络钓鱼这种事太常见了，也许不必更多解释，点击了这篇文章的大多数人应该都能有识别钓鱼的能力。在上面挪威实验的例子中，研究人员用一个假的免费汉堡的广告来钓鱼，这是要下载一个应用程序到受害者的智能手机，从而入侵。如果受害人贪便宜，就可以使攻击者能够从被感染的手机中操控汽车 —— 一辆不折不扣的特斯拉 Model S。令人震惊。

不要惊慌

虽然有人可以通过黑客技术进入您的汽车，或者最糟糕的是，能够控制关键系统，这个可能性的确很可怕，但不要惊慌。

现实世界的威胁似乎更多情况下只是来自小偷闯入并拿走东西。目前他们还可能在您行车中途关闭引擎，但是，很快他们就可以在您不知

情的情况下把您的车开走。不仅会让您失去财产还会制造恐慌。

联网汽车的优势和劣势并存。一方面，它可以为用户提供非常有用的信息，包括发动机性能跟踪和维护，并为制造商改进未来的车型提供微妙的数据。它们还有助于防止事故的发生，并为从故障到寻找最近的加油站等任何事提供车内的帮助。而另一方面，您可能会面临数据被盗的问题，以及被入侵操控的危险。

汽车数字化的速度只会越来越快；内置诊断、工具和附加设备等等，将继续发展和专业化。制造商需要认真思考未来可能提供的车辆的潜在漏洞。

如今的汽车和轻型卡车都装载了有利于汽车黑客攻击的无线入口。虽然目前风险还较低，但是，当您决定购买新车时，肯定值得考虑这个问题。

[image]
[image]

单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

[image] 关键词	大规模监视 监视资本主义 自卫
[image] 关联	[image]数字技术限制和最佳实践
[image] 创建时间	2021年6月10日
[image] **Description**	技术直觉

这里是一份手册，关于生活在目前这个世界中您需要知道的自己的处境 —— 从在线到现实。它是对这个反乌托邦世界的一个汇总，人们应该首先清楚地知道自己正在面对什么，下一步才是思考如何防御

- Table of Contents

介绍
第一方与第三方跟踪
他们都了解了关于您的什么
第1部分：跟踪者如何将数据与具体的人联系起来？
网络上的身份标识
1、请求的背后
2、身份标识自动共享
3、Cookies
4、IP地址
5、TLS状态
跟踪器创建的标识符
1、本地存储“Cookie”和 IFrame
2、指纹识别
移动设备上的身份标识
1、电话号码
2、硬件标识符：IMSI和IMEI

3、广告ID
4、MAC地址
真实世界中的身份标识
1、车牌
2、面部生物识别
3、信用卡/借记卡
随时间的推移被关联的标识符
第二部分：跟踪网络是什么样的？
软件中的跟踪：网站和应用程序
1、广告网络
2、分析和跟踪像素
3、嵌入式媒体播放器
4、社交媒体小部件
5、验证码
6、会话重播服务
被动的、真实世界中的跟踪
1、WiFi热点和无线信标
2、车辆跟踪和ALPR
3、人脸识别监视相机
4、支付处理器和金融科技
5、追踪和企业权力
第3部分：定位，代理和实时出价
1、实时出价
网络上的实时出价工具：Cookie同步
移动应用中的实时出价
2、群体定位和相似受众
3、数据经纪人
数据使用者
1、定向广告
2、政治运动和利益集团
3、讨债者、赏金猎人和欺诈调查员
4、城市、警察部门和间谍机构
第4部分：反击
在手机上
现实中

[image]

介绍

跟踪器隐藏在当今互联网的几乎每个角落，准确说是，现代生活中的几乎每个角落。

- 平均每个网页都与数十个第三方共享数据；
- 普通的移动应用程序也会这样做，并且许多应用程序即使您不使用它们时也会收集您的高度敏感的信息，例如位置和通话记录。
- 跟踪也可以进入物理世界。购物中心使用自动车牌读取器来跟踪其停车场的交通，然后与警察部门共享这些数据。
- 针对音乐会组织者和任何政治活动的监视使用蓝牙和WiFi信标对所在区域内的任何人进行定位。
- 零售商店使用面部识别来识别客户，并投放有针对性的广告....

简单说，无时无刻地，您一直在被窥探、被收集、被出售，当然也同时被出卖 —— 这些数据会在任何状况下交给警察和间谍，您随时可能蹲冤狱。并且这些被收集的数据随时可能被骇客泄漏，任何恶意者都可以用它们来迫害您。

普通用户看不到这种监视背后的技术公司、数据经纪人和广告商，以及推动该监视的技术究竟是什么样。这些公司建立了一个单向镜大厅：您只能看到社交媒体反映的应用程序，网页，广告和您自己。但是在玻璃后面的阴影中，跟踪器会悄悄地记录您所做的几乎所有事。

这些跟踪器不是无所不知的，但是它们是广泛且不加区分的。他们收集和导出的数据并不完美，但是非常敏感。

本文将重点关注公司的 “第三方” 跟踪，即：用户不希望与之交互的公司收集个人信息的行为。将阐明第三方跟踪背后的技术方法和商业惯例。希望本文能够揭开第三方跟踪的基本面，说明问题的范围，并帮助人们提出反击现状的方法。

第一方与第三方跟踪

当人们使用服务时，互联网上所有科技巨头公司都会收集大量的数据，他们就是这样发财的。Facebook 知道您的朋友是谁、您 “喜欢” 什么，以及您在新闻源上阅读的内容种类；Google 知道您的想法、您想知道什么、以及任何时候的去向；亚马逊知道您购买的商品、偏好、以及您住在哪 ……

这些公司通过自己的产品和服务收集的数据称为 “第一方数据”。

这些信息可能非常敏感，并且这些公司在隐私丑闻方面有着悠久的记录。

第一方数据有时是作为隐性或显式合同的一部分收集的：“选择使用我们的服务，并且您同意让我们使用在执行操作时收集的数据”。越来越多的用户开始理解，所有免费的服务都是把你当作商品出售的。

但是，即便您没有使用他们的服务，也同样会被这些寡头公司收集。

例如，Facebook 通过其无形的 “转换像素” 收集任何其他网站和应用程序上的用户信息；同样，谷歌使用位置数据来跟踪用户对实体店的访问 ……

而千千万万的其他数据中介、广告商和其他跟踪器则潜伏在您的日常网页浏览和设备使用的背景中。这就是所谓的 “第三方追踪”。如果没有经过训练的眼睛，第三方跟踪更难识别，而且几乎不可能完全避免。

他们都了解了关于您的什么

很多消费者都熟悉自己的电子设备最明目张胆的侵犯隐私的潜力。每部智能手机都是一个袖珍的GPS追踪器，通过互联网不断向未知的各方广播其位置。任何带有摄像头和麦克风的互联网连接设备都有转化为秘密窃听装置的内在风险。而风险是真实存在的：位置数据在过去曾被严重滥用。亚马逊和谷歌都曾允许员工收听他们的家庭监听设备 Alexa 和 Home 所录制的音频。而笔记本摄像头也曾被学校用来监视在家的学生。

但这些比较知名的监控渠道并不是最常见的，甚至不一定是威胁最大的。尽管我们每个人醒着的许多时间都是在电子设备的互联网连接摄像头的视野中度过的，但它们在没有用户明确意图的情况下记录任何东西的情况依旧罕见。而正如本文其余部分将显示的那样，追踪者从成千上万个不那么引人注目的数据来源中了解到的信息已经足够多了。

请注意：虽然 Facebook 没有通过手机监听你，但这只是因为它已经不需要这么做。

请记住：对您的隐私人权最普遍的威胁是缓慢、稳定、无情地积累有关您生活方式点点滴滴的相对平凡的数据点。这包括浏览历史、应用使用、购买和地理位置数据等等一切。

这些看似不起眼的部分可以组合成一个特别有启示性的完整图谱。追踪器将您的每一步操作的数据整合成庞大的行为档案，可以揭示政治派别、宗教信仰、性取向和性生活、种族和民族、教育水平、收入阶层、购买习惯、以及身体和心理的健康状况。

行为定位广告是利用用户的行为数据来预测他们喜欢什么，他们如何思考，以及他们可能购买什么的做法，它推动了大部分第三方跟踪行业的发展 —— 这就是监视资本主义的工作方式。虽然行为广告商有时可以获得精确的信息，但他们经常处理的是一概而论和“聊胜于无”的统计性猜测。

这样的结果只会让你看到完全不需要的广告。

但是，您需要知道，无论追踪者的推断是否正确，他们收集的数据都是过度侵犯性的和非常危险的，他们基于这些数据做出的任何决定都会造成具体的伤害。

第1部分：跟踪者如何将数据与具体的人联系起来？

大多数第三方跟踪是为了建立真实个人的详细档案。这意味着每次追踪者收集信息时，都需要一个标识 —— 它可以用这个身份标识将信息与特定的人联系起来。

有时，追踪者会间接地这样做：将收集到的数据与特定的设备或浏览器相关联，而这些设备或浏览器随后又可能与一个具体的人或一小部分人（如一个家庭）相关联。

为了找到具体的真实的个人，追踪者需要独特的、持久和可用的身份标识。换句话说，追踪者正在寻找：

(1) 仅指向你或你的设备的信息，

(2) 不会改变的信息，

(3) 易于访问的信息。

一些潜在的身份标识符合所有这三个要求，但追踪者仍然可以只选中这三个框中两个即可满足需求。追踪者可以将多个较弱的识别线索组合起来，创建一个强大的身份识别依据。

符合上述所有3个条件的身份标识是，比如一个名字、一个电子邮件

或一个电话号码。

也可能是追踪器本身分配给你的 “名字”，比如 “af64a09c2” 或 “921972136.1561665654”。

对追踪器来说，最重要的是标识指向你，而且只指向你。

随着时间的推移，它可以建立一个足够丰富的关于被称为比如 “af64a09c2” 的人的档案 —— 此人住在哪里，他读了什么，他买了什么 —— 传统的名字是不必要的。

追踪者可以使用人工标识，比如 cookie 和移动广告ID，向用户发送有针对性的信息。而不与真实姓名挂钩的数据也同样敏感：个人信息的 “匿名” 档案几乎总是可以被链接到真实的人身上。

BACK [image]即使数据是匿名的，您的身份仍然可以被识别

有些类型的标识符，如 cookie，是您使用的技术中内置的功能。其他类型的标识符（如浏览器指纹）则是由这些技术的工作方式产生的。本节将分析网络和移动应用程序中的跟踪器如何能够识别和归属数据点。

本节将描述第三方跟踪器可以使用的标识的代表性样本。本节并不意味着详尽无遗；追踪器识别用户的方法比我们希望涵盖的更多，而且随着技术的发展，新的标识方式会不断出现。下面的表格简要介绍了每一种身份标识的独特性、持久性和可用程度。

网络上的身份标识

浏览器是大多数人与网络互动的主要方式。每次您访问一个网站时，该网站上的代码就会使您的浏览器向隐藏的第三方发出几十甚至几百个请求。每个请求都包含多条信息，可以用来跟踪你。

1、请求的背后

浏览器与您所交互的网站服务器之间传输的几乎每一条数据都是以HTTP 请求的形式进行的。基本上，您的浏览器通过向网络服务器发送一个特定的URL来请求它提供内容。

网络服务器可以用内容（如文本或图像）或简单的确认收到您的请求来回应。它也可以用 cookie 来回应，cookie 可以包含一个用于跟踪目的的唯一标识符。

您访问的每个网站都会启动几十个或几百个不同的请求。您在浏览器地址栏中看到的URL是第一个请求的地址，但在后台还会有数百个其他请求。这些请求可以用于加载图像、代码和样式，或者仅仅是为了共享数据。

Parts of a URL. The domain tells your computer where to send the request, while the path and parameters carry information that may be interpreted by the receiving server however it wants.

[image]

URL本身包含几个不同的信息。首先是域名，比如 “nytimes.com”。这告诉您的浏览器要连接到哪个服务器。其次是路径，域名末尾的一个字符串，如 “/section/world.html”。nytimes.com 的服务器会选择如何解释该路径，但它通常会指定一个要提供的内容 —— 本例中是世界新闻部分。

最后，一些URL的结尾有 “?key1=value1&key2=value2” 形式的参数。这些参数通常带有关于请求的额外信息，包括用户进行的查询、关于页面的上下文和跟踪标识符。

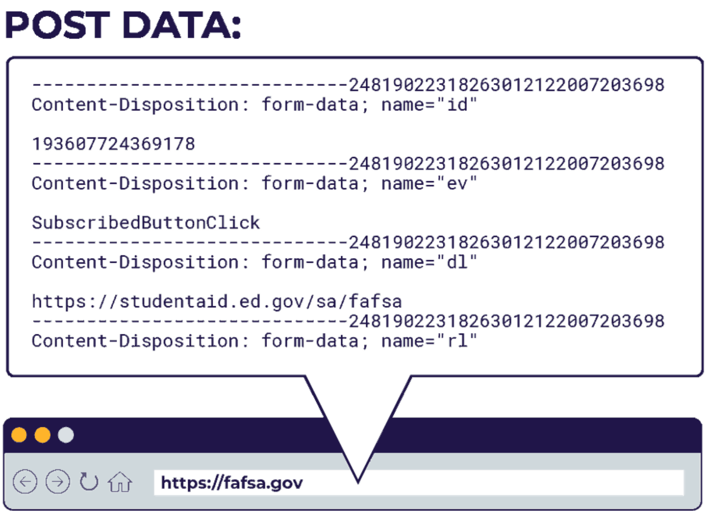
[image] 请求的路径

URL并不是被发送到服务器的全部。还有一些HTTP头字段，其中包含有关请求的额外信息，如您的设备的语言和安全设置，“referring”、URL 和 cookies。

例如，User-Agent 头可以识别您的浏览器类型、版本和操作系统。还有关于连接的低级信息，包括IP地址和共享加密状态。

有些请求以POST数据的形式包含更多可配置的信息。POST请求是网站共享数据的一种方式，这些数据块太大或太笨重，无法容纳在URL中。它们可以包含任何内容。

其中一些信息，如URL和POST数据，是专门为每个单独的请求定制的；其他部分，如您的IP地址和任何 cookies，由您的机器自动发送。几乎所有的信息都可以用于跟踪。



请求中包含的数据

上面的动图显示了直接从正常版本的 Firefox 中收集的数据。

如果您想自己检查一下也可以。所有主流的浏览器都有一个 “检查器” 或 “开发者” 模式，它允许用户查看幕后发生的事，包括所有来自特定标签页的请求。

在 Chrome 和 Firefox 中，你可以通过 Crtl+Shift+I（或Mac上的⌘+Shift+I）进入这个界面。在 “网络” 选项卡中，有一个特定页面发出的所有请求的日志，您可以点击每一个请求，查看它的去向和包含

的信息。

2、身份标识自动共享

在每次请求时，一些可识别的信息都会自动共享。这是必要的，比如IP地址，这是互联网的基础协议所要求的，或者说它就是这么设计的，比如 cookies。追踪者并不需要做更多的事，只需要触发一个请求，任何请求，就可以收集这里描述的信息。

[image] 每次您通过输入网址或点击链接访问网站时，您的计算机都会向该网站的服务器（即"第一方"）发送请求。同时，它可能还会向其他服务器发送数十甚至数百次请求，其中许多服务器都可能追踪您的行踪。

3、Cookies

第三方跟踪最常用的工具是 HTTP Cookie。Cookie 是存储在浏览器中的一小段文字，与特定的域相关联。Cookie 的发明是为了帮助网站所有者确定用户是否曾经访问过他们的网站，这使得它们成为行为跟踪的理想选择。

下面是它们的工作原理。

当您的浏览器第一次向一个域名（比如 www.facebook.com）发出请求时，服务器可以在其回复中附加一个 Set-Cookie 消息头。这将告诉您的浏览器存储网站想要的任何值 —— 例如，c_user: “100026095248544”（从作者的浏览器中提取的实际 Facebook cookie）。

以后每次您的浏览器向 www.facebook.com 提出请求时，就会把之前设置的 cookie 一起发过来。这样一来，每次 Facebook 收到请求时，它就会知道请求来自哪个个人用户或设备。

[image] 当浏览器首次向新服务器发送请求时，服务器可通过返回包含“Set-Cookie”标头的响应，在浏览器中存储一个用于追踪的Cookie。

不是每一个 cookie 都是追踪器。Cookie 也是您不必每次访问网站时都要登录的原因，也是您在购物过程中离开网站时购物车不会清空的原因。Cookies 只是一种从您的浏览器到您正在访问的网站共享信息的手段。然而，它们被设计成能够携带跟踪信息，第三方跟踪是它们最臭名昭著的用途。

幸运的是，用户可以对浏览器处理 cookies 的方式进行大量控制。此外，Safari 和 Firefox 最近也开始限制他们认为是追踪器的域对第三方 cookies 的访问。

由于追踪器与阻止它们的方法之间的这种“猫鼠游戏”，第三方追踪开始从单纯依靠 cookies 来识别用户身份转变为依靠其他标识信息。

Cookie 始终是唯一的，它们通常会持续存在，直到用户手动清除它们。在未经修改的 Chrome 浏览器版本中，跟踪器始终可以使用 Cookies，但在 Safari 和 Firefox 中，许多跟踪器不再使用第三方 Cookies。用户可以随时使用浏览器扩展程序自行阻止 Cookie。

4、IP地址

您在互联网上发出的每个请求都包含您的IP地址，这是一个对您的设备来说独一无二的临时标识符。

虽然它是唯一的，但它不一定是持久的：每当您移动到一个新的网络时（例如，从家里到公司再到咖啡店），您的IP地址就会改变。由于IP地址的工作方式，即使您一直连接到同一个网络，它也可能会改变。

目前广泛使用的IP地址有两种，即 IPv4 和 IPv6。世界上只有大约40亿个IPV4地址。它很老了，是曾经为只有几百家机构使用的互联网而设计的。即使如此，目前超过70%的互联网流量仍然使用 IPv4。

因此，消费者设备使用的 IPv4 地址不断被重新分配。当设备连接到互联网时，其互联网服务提供商（ISP）会给它“租”一个 IPv4 地

址，这样，设备就可以在几个小时或几天内使用一个地址。当租约到期时，ISP可以决定延长租约或授予它一个新的IP。如果一个设备长期在同一个网络上，它的IP可能每隔几个小时就会改变一次，也可能几个月都不改变。

IPv6 地址不存在同样的稀缺性问题，它们不需要改变，但由于技术标准的隐私保护扩展，大多数设备每隔几小时或几天就会产生新的随机IPv6地址。

这意味着 IPv6 地址可用于短期跟踪或链接其他标识符，但不能作为独立的长期身份标识使用。

IP地址本身并不是完美的标识符，但如果有足够的数据，追踪者依旧可以利用它们来创建用户的长期档案，包括映射设备之间的关系。

您可以通过使用可信的 VPN 或 Tor 浏览器来隐藏您的IP地址，以防止第三方追踪者的追踪。

5、TLS状态

今天，网络上的大部分流量都是使用传输层安全性协议（TLS）加密的。任何时候你连接到一个以 “https://” 开头的URL，都是在使用TLS连接。这是一件好事。TLS和HTTPS提供的加密连接可以防止ISP、黑客和政府监视网络流量，并确保数据在到达目的地的途中不会被拦截或修改。

然而，它也为追踪者开辟了识别用户的新途径。TLS会话ID和会话记录单是有助于加快加密连接的加密标识符。当您通过HTTPS连接到服务器时，您的浏览器会与服务器启动一个新的TLS会话。

服务器可以向浏览器发送一个会话记录单，对一些共享的加密状态进行编码，而不是每次重新连接时在服务器和浏览器之间执行一个完整的加密 “握手”。下次您连接到同一台服务器时，您的浏览器就会发送会话记录单，让双方跳过握手。唯一的问题是，会话记录单可以被追

踪者利用，作为唯一的身份标识。

TLS会话跟踪最近才在一篇学术论文中引起公众注意，目前还不清楚它在实际中的应用有多广泛。

像IP地址一样，会话记录单总是唯一的。它们是可用的，除非用户的浏览器被配置为拒绝它们，就像Tor那样。服务器运营商通常可以配置会话记录单，以持续一个星期，但浏览器会在一段时间后重置它们。

跟踪器创建的标识符

有时，基于网络的跟踪器希望使用的标识不仅仅是IP地址（不可靠且不持久）、cookies（用户可以清除或阻止）或TLS状态（数小时或数天内失效）。为此，追踪者需要付出更多的努力。他们可以使用 JavaScript 在本地存储中保存和加载数据，或者执行浏览器指纹追踪。

1、本地存储 “Cookie” 和 IFrame

本地存储是网站在浏览器中长期存储数据的一种方式。本地存储可以帮助基于网络的文本编辑器保存您的设置，或允许在线游戏保存您的进度。与 Cookie 一样，本地存储允许第三方跟踪器在您的浏览器中创建和保存唯一标识符。

同样和 cookies 一样，本地存储中的数据也与特定的域相关联。这意味着如果 example.com 在您的浏览器中设置了一个值，只有 example.com 的网页和 example.com 的 IFrame 可以访问它。

一个IFrame就像网页中的一个小网页。在 **IFrame** 内，第三方域可以做几乎所有第一方域可做的事。

例如，嵌入的 YouTube 视频是使用 IFrame 构建的；每次您在

YouTube 以外的网站上看到一个 YouTube 视频时，它都是在一个小页面内运行。在大多数情况下，您的浏览器把 YouTube IFrame 当作一个成熟的网页，允许它读写 YouTube 的本地存储。

当然，YouTube 使用该存储空间来保存一个唯一的 “设备标识符”，并跟踪任何嵌入视频的页面上的用户。

本地存储 “cookie” 是独一无二的，它们会一直存在，直到用户手动清除其浏览器存储。它们只适用于能够在第三方 IFrame 内运行 JavaScript 代码的追踪器。并非所有的 **cookie** 阻止措施都会考虑到本地存储 **cookie**，因此本地存储 **cookie** 有时可能会提供给那些正常 **cookie** 访问被阻止的跟踪器。

2、指纹识别

浏览器指纹是最复杂、最隐蔽的网络跟踪形式之一。浏览器指纹由一个或多个属性组成，这些属性单独或组合在一起时，可以唯一地识别单个设备上的单个浏览器。

通常情况下，进入指纹的数据是浏览器不得不暴露的东西，因为这是它与网络交互方式的一部分。这些数据包括每次浏览器访问网站时随请求发送的信息，以及通过在页面上运行 JavaScript 可以发现的属性。

例如，您的屏幕分辨率、您安装的软件的具体版本以及您的时区。浏览器向您访问的网站暴露的任何信息都可以被用来建立浏览器指纹。

指纹的可靠性是一个积极研究的课题，必须在不断发展的网络技术的背景下加以衡量。然而，新技术显然增加了独特识别的可能性，使用指纹的网站数量也在增加。最近的一份报告发现，在美国人访问的前500名网站中，至少有三分之一采用了某种形式的浏览器指纹。指纹在网站上的普及率也因网站的类别不同而有很大差异。

研究人员发现画布指纹技术对浏览器识别特别有效。HTML画布是

HTML5的一个功能，它允许网站在网页内部渲染复杂的图形。它被用于游戏、艺术项目以及一些最漂亮的网站。因为它是如此复杂和性能密集，所以它在每个不同的设备上的工作方式有点不同。画布指纹就是利用了这一点。

[image] 画布指纹识别

跟踪器可以创建一个用户不可见的 “画布” 元素，使用 JavaScript 渲染一个复杂的形状或一串文本，然后提取数据，了解画布上每个像素到底是如何渲染的。电脑上安装的操作系统、浏览器版本、显卡、固件版本、图形驱动程序版本和字体都会影响最终的结果。

当追踪器将多个特征结合在一起拼接成一个整体时，就能最有效地识别一个浏览器。其他特征 —— 比如您的语言、时区或浏览器设置 —— 结合起来就可以识别您的身份。这些简单的信息组合比您猜想的要有效得多。

指纹往往是独一无二的，但并不总是独一无二。一些浏览器，如 Tor，是专门设计的，因此它们的用户更有可能看起来一样，这就消除或限制了浏览器指纹的有效性。你无法通过设置来 “重置” 你的指纹。而且指纹通常可以被任何能在您的浏览器中运行 JavaScript 的第三方获得。

移动设备上的身份标识

智能手机、平板电脑和电子书阅读器的网络浏览器通常与桌面浏览器的工作方式相同。这意味着，这些类型的连接设备很容易受到上节所述的所有类型的跟踪。

然而，移动设备在两个大方面有所不同。首先，用户通常需要用苹果、谷歌或亚马逊账户登录，才能充分利用设备的功能。这就将设备标识符与账户身份联系起来，使那些强大的企业行为者更容易对用户行为进行描述。

例如，为了在谷歌地图中保存您住所和工作单位的地址，您需要开启

谷歌的 “网络和应用活动”，于是它就可以利用你的位置、搜索历史和应用活动来定位广告。

其次，同样重要的是，大多数人在移动设备上的大部分时间是在浏览器之外的应用程序中度过的。应用程序中的追踪器不能像基于网络的追踪器那样访问 cookies。但是，通过利用移动操作系统的工作方式，应用程序跟踪器仍然可以访问独特的标识符，让他们将具体活动与你的设备联系起来。

此外，手机 —— 特别是那些运行Android和iOS操作系统的手机 —— 可以访问一组独特的标识符，用于追踪。

在移动生态系统中，大多数跟踪都是通过第三方软件开发包SDK的方式进行的。SDK是一个代码库，应用程序开发人员可以选择将其包含在他们的应用程序中。

在大多数情况下，SDK的工作原理就像上文讨论的第三方利用的网络资源一样：它们允许第三方了解你的行为、设备和其他特征。一个想要使用第三方分析服务或为第三方广告提供服务的应用开发者从谷歌或 Facebook 等公司下载一段代码，然后将该代码包含在其应用的发布版本中。因此，第三方代码可以访问应用程序的所有数据 —— 包括在授予该应用程序的任何权限（例如位置或摄像头访问权限）之后受保护的数据。

在web上，浏览器对 “第一方” 和 “第三方” 资源进行了区分。这使得他们可以对第三方内容进行额外的限制，比如阻止他们访问浏览器的存储空间。但在移动应用中，这种区分并不存在。你不能在授予一个应用程序特权的同时，不授予其内部运行的所有第三方代码获得相同的特权。

1、电话号码

电话号码是最古老的独特数字标识符之一，也是最容易理解的标识符之一。每个号码对特定的设备来说都是独一无二的，而且号码不会经常变化。用户被鼓励分享他们的电话号码，原因多种多样（例如，账

户验证、电子收据和实体店的忠诚度计划等等）。

因此，数据经纪人经常收集和出售电话号码。但是，电话号码并不容易从应用内部获取。在安卓系统上，电话号码只有被授予一定权限的应用程序中的第三方追踪者才能获得。iOS系统则完全阻止应用程序访问用户的电话号码。

电话号码是唯一且持久的身份标识，但在大多数应用中，第三方追踪者通常无法获取。

2、硬件标识符：IMSI和IMEI

每一台能够连接到移动网络的设备都会被分配一个唯一的标识符，称为国际移动用户识别码（IMSI）。IMSI号码由移动运营商分配给用户，并存储在SIM卡上，普通用户如果不更换SIM卡，就无法更改IMSI。这使得它们成为追踪的理想选择。

同样，每个移动设备的硬件中都有一个“内置”的国际移动设备识别号（IMEI）。您可以更换您的SIM卡和电话号码，但如果不购买新的设备，你就无法更换IMEI。

IMSI号码在你每次连接到手机信号塔时都会与手机供应商共享；当你在世界范围内移动时，你的手机会向附近的信号塔发送寻呼，以获取有关网络状态的信息。你的手机运营商可以使用这些信息来跟踪你的位置（不同程度的准确性）。这不完全是第三方跟踪，因为它是由与您有关系的手机公司实施的，但无论如何，许多用户可能没有意识到它的发生。

在手机上运行的软件和应用程序也可以访问IMSI和IMEI号码，但不那么容易。移动操作系统在权限背后锁定了对硬件标识符的访问，用户必须批准这些权限，并且以后可以撤销。例如，从 Android Q 开始，应用程序需要请求“READ_PRIVILEGED_PHONE_STATE”权限才能读取不可重置的ID。

在iOS上，应用程序根本不可能访问这些标识符。这使得其他标识符对于大多数基于应用的第三方追踪器来说，成为更有吸引力的选择。

与电话号码一样，IMSI和IMEI号码也是唯一且持久的，但并不容易获得，因为大多数追踪器很难访问它们。

3、广告ID

广告ID是一个长长的、随机的字母和数字组成的字符串，可以唯一地识别移动设备。广告ID不是任何技术协议的一部分，而是内置在 iOS 和 Android 操作系统中的。

手机上的广告ID类似于网络上的 cookies。广告ID不像 cookies 那样由浏览器存储并与不同网站上的追踪器共享，而是由手机存储并与不同应用中的追踪器共享。广告ID存在的唯一目的是帮助行为广告商在设备上的不同应用中链接用户活动。

与 IMSI 或 IMEI 号码不同，广告 ID 可以更改，在 iOS 上可以完全关闭。在iOS和Android上，广告ID都是默认启用的，所有应用都可以使用，无需任何特殊权限。广告ID不会重置，除非用户手动重置。

谷歌和苹果都鼓励开发者使用广告ID进行行为特征分析，以代替IMEI或电话号码等其他标识符。

表面上看，这让用户对自己的追踪方式有了更多的控制权，因为如果用户选择，他们可以手动重置自己的标识符。然而，在实际操作中，即使用户费尽心思去重置他们的广告**ID**，追踪者也很容易通过使用其他标识符，如**IP**地址或应用内存储来识别他们的身份。

安卓的开发者政策指示追踪者不要从事这种行为，但平台没有技术保障措施来阻止这种行为。2019年2月，一项研究发现，Play商店中超过1.8万个应用违反了谷歌的政策。

广告 ID 是唯一的，默认情况下所有应用程序都可以使用。它们会一

直存在，直到用户手动重置它们。这使得它们成为对诡异的追踪者来说非常有吸引力的标识符。

4、MAC地址

每个可以连接到互联网的设备都有一个硬件标识符，称为媒体访问控制（MAC）地址。MAC地址用于设置两个无线设备之间通过WiFi或蓝牙的初始连接。

各种设备都会使用MAC地址，但在移动设备上，与之相关的隐私风险更高。你通过互联网与之交互的网站和其他服务器实际上无法看到你的MAC地址，但你所在区域的任何网络设备都可以。事实上，您甚至不需要连接到网络，它就能看到你的MAC地址，在附近就足够了。

下面是它的工作原理。为了找到附近的蓝牙设备和WiFi网络，您的设备会不断地发送被称为探测请求的无线电信号。每个探测请求都包含您的设备的唯一MAC地址。如果该地区有WiFi热点，它将听到探针，并发送回自己的“探针响应”，通过设备的MAC地址进行寻址，并提供有关如何连接的信息。

但该区域内的其他设备也能看到并拦截到探测请求。这意味着，企业可以设置无线“信标”，静静地监听附近的MAC地址，然后利用这些数据来追踪特定设备在一段时间内的移动情况。

只要在足够多的地方设置足够多的信标，公司就可以追踪用户在商店周围或在一个城市里的移动。他们还可以识别两个人何时在同一地点，并利用这些信息建立一个社交图谱。

[image] 为了发现附近的蓝牙设备和WiFi网络，您的设备会持续发送名为探测请求的短距离无线电信号。每个探测请求都包含设备唯一的MAC地址。

这种跟踪方式可以通过MAC地址随机化来挫败。在探测请求中，您的设备可以编造一个新的、随机的、“欺骗性的”MAC地址，而不是共享其真实的、全球唯一的MAC地址，以便每次进行广播。这使得被动跟踪器无法将一个探测请求链接到另一个探测请求，或将它们链接到

特定设备。幸运的是，最新版本的iOS和Android都默认包含MAC地址随机化功能。

MAC地址追踪对于笔记本电脑、老式手机和其他设备来说，仍然是一个风险，但行业正趋向于更多的隐私保护规范。

硬件MAC地址是全球唯一的。它们也是持久的，在设备的生命周期内不会改变。它们不容易被应用程序中的追踪器使用，但被动追踪器可以使用无线信标。由于现在许多设备默认情况下会混淆MAC地址，因此它们正在成为被动跟踪的一个不太可靠的标识符。

真实世界中的身份标识

许多电子设备的标识符可以被用户重置、混淆或关闭。但现实世界中的身份标识就不同了：开车时（包括停车时）遮住车牌是违法的，而改变脸部和指纹等生物标识符则几乎不可能。

1、车牌

每一辆车都被法律要求有一个与其现实世界身份相联系的车牌。就追踪识别而言，车牌号是最好的东西。它们很容易被发现，而且遮盖非法。它们不容易被改变，而且无论人们走到哪里都可以被跟踪。

自动车牌阅读器 ALPRs，是一种特殊用途的摄像头，可以自动识别和记录过往车辆的车牌号码。ALPR可以安装在固定的地点，比如繁忙的十字路口或商场停车场，也可以安装在其他车辆上，比如警车。私营公司经营ALPR，利用它们积累大量的旅客位置数据，并将这些数据卖给其他企业 —— 包括警察。

不幸的是，对于开车的人来说，ALPRs的追踪基本上是不可避免的。由于大多数ALPRs都是在公共场所运行，所以要避开这些设备本身是非常困难的。

车牌是独一无二的，任何人都可以看到车辆，而且非常持久。它们是警察和第三方追踪者收集车辆及其驾驶员数据的理想标识符。

2、面部生物识别

面孔是另一类对第三方追踪者极具吸引力的独特标识符。面孔是独一无二的，而且极不方便更改。如今遮住脸也是违法的。

每个人的脸都是独一无二的，可用的，也是持久的。然而，目前的人脸识别软件有时会把不同的人混为一谈。此外，研究表明，算法在识别有色人种、女性和老年人时，更容易犯这类错误。

面部识别已经得到了广泛的部署，但我们可能才刚刚开始感受到它的影响程度。面部识别摄像头已经出现在商店、街角，以及在所谓的智能眼镜上。如果没有强有力的隐私法规，普通人几乎没有办法反击通过面部识别进行的无孔不入的追踪和剖析。

3、信用卡/借记卡

信用卡号是另一个极好的长期标识符。虽然它们可以被循环使用，但大多数人更换信用卡号码的频率并不像清除 cookie 那样频繁。此外，信用卡号与真实姓名直接挂钩，任何在交易中收到您的信用卡号的人也会收到您的法定姓名。

大多数人可能不明白的是，每一笔信用卡交易都有大量的隐藏第三方参与。如果你在当地的商店买了一个小部件，商店可能会与提供办卡服务的支付处理商签约。该交易还必须经过您的银行以及信用卡供应商的银行的验证。

支付处理商又可能雇用其他公司来验证其交易，而所有这些公司都可能收到有关购买的信息。银行和其他金融机构受到法律监管，要求他们披露用户数据的共享方式，并给予用户选择不共享的权利。然而，其他金融科技公司，如支付处理商和数据聚合商，受到的监管要少得多。

随时间的推移被关联的标识符

通常情况下，跟踪器不能依靠单一的标识符来作为与用户的稳定链接。IP地址会发生变化，人们会清除 cookie，广告ID可能会被重置，更精明的用户可能会使用一次性电话和电子邮件地址。

即便如此，跟踪者也不会放弃。他们通常会将多个身份标识组合起来，创建一个统一的档案。这样一来，当一个标识或另一个标识发生变化时，他们也不太可能失去对用户的追踪，而且随着时间的推移，他们可以将旧的标识符与新的标识符联系起来。

追踪者在这里有一个优势，因为有很多不同的方法来识别用户。如果用户清除了 Cookie，但他们的IP地址没有改变，那么将旧的 Cookie 与新的 Cookie 联系起来是轻而易举的。

如果他们从一个网络转移到另一个网络，但使用相同的浏览器，浏览器指纹可以将他们的旧会话链接到新会话。

如果他们阻止第三方 cookie，并使用难以指纹追踪的浏览器，跟踪者可以使用第一方cookie共享与TLS会话数据相结合，以建立用户行为的长期档案。

在这场猫鼠游戏中，追踪者比个人用户具有技术优势。

[image]

第二部分：跟踪网络是什么样的？

为了跟踪你，大多数跟踪公司需要说服网站或应用程序开发人员在其产品中加入自定义跟踪代码。这可不是一件小事：追踪代码可能会减慢软件的速度，惹恼用户，并引发GDPR等法律的监管。

然而，最大的追踪网络覆盖了网络和应用商店的大片区域，一直从数百万个不同的来源收集数据。在物理世界中，跟踪器可以在广告牌、零售店和商场停车场中找到。那么，追踪器是如何以及为什么如此广泛地存在呢？

Top trackers on the Web, ranked by the proportion of web traffic that they collect data from. Google collects data about over 80% of measured web traffic. Source: WhoTracks.me, by Cliqz GBMH.

[image]

软件中的跟踪：网站和应用程序

1、广告网络

[image]

第三方追踪背后的主导市场力量是广告行业，下文第三部分将讨论。因此，在线广告是数据收集的主要载体之一也就不足为奇了。

在最简单的模型中，一个单一的第三方广告网络在一些网站上提供广告。每个与广告网络合作的出版商必须在其网站上包含一小段代码，该代码将从广告服务器加载广告。

每次用户访问合作网站时，都会触发对广告服务器的请求，从而让广告服务器在用户的浏览器中设置第三方 cookies，并跟踪用户在整个网络中的活动。

同样，广告服务器可能会提供一个广告托管软件开发工具包（SDK），供移动应用开发者使用。每当用户打开使用SDK的应用时，该应用就会向广告服务器发出请求。这个请求可以包含用户设备的广告ID，从而使广告服务器能够对用户在不同应用中的活动进行描述。

实际上，在线广告生态系统更加复杂。广告交易市场为网页上的单个

广告展示举办 “实时拍卖”。在这个过程中，他们可能会从其他多个第三方广告供应商那里加载代码，并可能与许多参与拍卖的潜在广告商共享每个展示的数据。您看到的每个广告可能正在与几十个跟踪器共享数据。

2、分析和跟踪像素

跟踪代码通常不与用户可见的任何东西相关联，比如第三方广告。在网络上，很大一部分跟踪是看不见的。这些 “跟踪像素” 被许多网络上最多产的数据收集器使用，包括谷歌分析、Facebook、亚马逊和DoubleVerify。

当网站所有者安装第三方的跟踪像素时，他们通常会以访问第三方收集的一些数据为交换条件。例如，谷歌分析和 Chartbeat 使用像素收集信息，并为网站所有者和出版商提供关于什么样的人正在访问他们的网站的分析。

再深入一个层次，像 Facebook 这样的广告平台还提供 “转换像素”，让发布者可以跟踪自己的第三方广告获得了多少点击量。

基于网络的分析领域的最大玩家也为移动应用提供类似的服务。Google Analytics 和 Facebook 是 Android 和 iOS 上最受欢迎的两个SDK。这些服务默默地收集移动应用的用户信息，然后与应用开发者分享部分信息。

移动第三方跟踪器通过提供分析或单点登录等有用的功能来说服应用开发者安装其SDK。SDK只是应用程序开发人员添加到其项目中的大块代码。当他们编译和发布一个应用时，第三方代码就会随应用一起发布。与基于Web的工具不同，移动应用中的分析服务不需要使用 “像素” 或其他技巧来触发第三方请求。

另一类跟踪器代表广告商工作，而不是第一方网站或应用程序。这些公司与广告商合作，监测他们的广告在哪里、如何、以及向谁提供服务。他们往往不与第一方出版商合作，事实上，他们的目标是收集出版商以及用户的数据。

DoubleVerify 是最大的此类服务之一。第三方广告商在投放广告的同时注入 DoubleVerify 代码，DoubleVerify 会估计每个展示是否来自真实的人类（而不是机器人），人类是否是广告商的目标对象，以及广告周围的页面是否 “品牌安全”。

根据其隐私政策，该公司会衡量 “广告在消费者浏览器中显示的时间” 和 “广告在消费者浏览器上的显示特征”。为了做到这一切，DoubleVerify 收集了用户浏览器的详细数据；它是迄今为止网络上最大的第三方浏览器指纹来源。

它收集位置数据，包括来自其他第三方来源的数据，试图确定用户是否在广告商所瞄准的地理区域观看广告。

该领域的其他公司包括 Adobe、Oracle 和 Comscore。

3、嵌入式媒体播放器

有时，第三方跟踪器会提供用户真正想看的内容。在网络上，嵌入第三方内容对于博客和其他媒体网站来说极为常见。一些例子包括 YouTube、Vimeo、Streamable 和 Twitter 等服务的视频播放器，以及 Soundcloud、Spotify 和播客流服务的音频小部件。

这些媒体播放器几乎总是在 IFrames 中运行，因此可以访问本地存储，并能够运行任意的 JavaScript。这使得它们也非常适合追踪用户。

4、社交媒体小部件

社交媒体公司为网站提供各种服务，如 Facebook “点赞” 按钮和 Twitter分享按钮。请记得 **Like** 和 **Share** 按钮可以像像素一样被用于跟踪：“按钮” 实际上是一个嵌入的图像，它触发了对社交媒体公司服务器的请求。

更复杂的小部件，如评论区，工作方式更像嵌入式媒体播放器。它们通常位于 IFrames 内部，更容易进入用户的浏览器。像媒体播放器一样，这些小部件能够访问本地存储和运行 JavaScript，以便计算浏览器指纹。

最后，最大的公司（尤其是 Facebook 和谷歌）向小公司提供账户管理服务，比如 “用谷歌登录”。这些被称为 “单点登录” 的服务对出版商有吸引力，原因有几个。比如 独立网站和应用程序可以将管理用户账户的工作卸载给大公司；用户需要记住的用户名/密码相对较少，也不需要经常经历恼人的注册/登录流程 …… 但是，对于用户来说，是要付出代价的：账户管理服务允许登录服务商作为第三方，跟踪用户在所有登录服务上的活动。登录服务是比像素等小玩意更厉害的跟踪器，因为它们迫使用户确认身份。

5、验证码

验证码是一种测试用户是不是机器人的技术。出版商在他们想要特别小心阻止自动流量的页面上安装这东西，比如注册表和可投放特别大的文件的页面。

谷歌的 ReCAPTCHA 是网络上最流行的验证码技术。每当连接到一个使用 recaptcha 的网站时，您的浏览器都会连接到一个*.google.com 域，以便加载验证码资源，并与谷歌共享所有相关的 **cookies**。这意味着其验证码网络是谷歌可以用来描述用户的另一个数据来源。

旧的验证码要求用户阅读乱码文字或点击比如自行车的图片，而新的 ReCAPTCHA v3 记录了 “与网站的互动”，并默默地猜测用户是否是人类。

ReCAPTCHA 脚本不会将原始的交互数据发回给谷歌。相反，它们会生成类似于行为指纹的东西，它总结了用户与页面的交互方式。

谷歌将其反馈到机器学习模型中，以估计用户是人类的可能性有多大，然后将该估计值返回给第一方网站。

除了让用户更方便之外，这个较新的系统还在两个方面给谷歌带来了好处。首先，它使大多数用户看不到 CAPTCHAS，这可能会使人们不太清楚谷歌（或任何人）正在收集他们的数据。其次，它利用谷歌庞大的行为数据集来巩固其在验证码市场的主导地位，并确保未来的任何竞争对手都需要他们自己的一部分交互数据以建立以类似方式工作的工具。

6、会话重播服务

会话重播服务是网站或应用程序所有者可以安装的工具，以便实际记录用户如何与他们的服务互动。这东西既可以在网站上操作，也可以在应用程序中操作。它们记录用户的按键、鼠标移动、点击、滑动和对页面的更改，然后允许第一方网站在事后 “重放” 个人用户的体验。

通常情况下，用户不会知道自己的行为被记录并与第三方共享。

这些令人毛骨悚然的工具带来了巨大的风险，敏感数据，如医疗信息、信用卡号码或密码，都将被记录和泄露。

会话重播服务的提供者通常会让客户自行将某些数据指定为禁区。但是对于客户来说，过滤掉敏感信息的过程是微妙的、费力、耗时，而且这与重放服务 “在几秒钟内就能设置好” 的承诺完全矛盾。

因此，独立审计发现，敏感数据最终依旧会出现在记录中，而会话重播服务提供商往往不能适当保护这些数据。

被动的、真实世界中的跟踪

1、WiFi热点和无线信标

许多消费类设备发出无线 “探针” 信号，许多公司安装了商业信标，

在物理世界的各个角落拦截这些探针。一些设备会随机分配它们在探针中共享的唯一MAC地址设备标识符，保护自己免受被动追踪，但并不是所有设备都会这样做。而连接到开放的**WiFi**网络或给应用蓝牙权限，总是会让设备打开追踪。

如上所述，WiFi热点、无线信标和其他无线电设备都可以用来“监听”附近的设备。像 Comcast（提供 XFinity WiFi）和谷歌（在星巴克和许多其他企业中提供免费WiFi）这样的公司在世界各地都安装了WiFi热点；仅 Comcast 就拥有超过1800万个 XFinity WiFi 安装。还有几十家你可能都没听说过的公司为咖啡店、餐厅、活动和酒店提供免费WiFi。

公司还付费在现实世界的企业和公共场所安装无线信标。在零售店周围、政治集会上、竞选活动现场以及路灯杆上都安装了支持蓝牙的信标。

无线信标能够在两个层面进行跟踪。首先，也是最令人关注的，无线信标可以被动地监控设备一直发出的“探针”。如果一个设备正在广播它的硬件MAC地址，公司就可以利用它们收集到的探针来追踪其用户在一段时间内的移动情况。

[image]

其次，当用户连接到WiFi热点或蓝牙信标时，热点或信标的控制器可以将设备的MAC地址与IP地址、Cookie 和广告ID等附加标识符连接起来。

许多WiFi热点运营商还使用登录页面来收集用户的真实姓名或电子邮件地址信息。

然后，当用户从该热点浏览网页时，运营商就可以收集所有来自用户设备的流量数据，就像**ISP**一样。

蓝牙信标的使用方式略有不同。手机允许应用程序在获得一定权限的情况下访问蓝牙接口。而拥有蓝牙权限的应用中的第三方追踪器可以自动连接到现实世界中的蓝牙信标，它们可以利用这些连接收集非常

详细的位置数据。

值得庆幸的是，现在 iOS 和 Android 设备都默认发送带有探针的混淆MAC地址。这就避免了上述第一种、被动式的追踪方式。

但手机并不是唯一具有无线功能的设备。笔记本电脑、电子阅读器、无线耳机，甚至汽车，都经常配备蓝牙功能。

这些设备中的一些并不具备新型号的智能手机所具备的MAC随机化功能，这使得它们很容易受到被动式位置跟踪的影响。

此外，即使是具有MAC随机化功能的设备，在实际连接到无线热点或蓝牙设备时，通常也会共享静态的MAC地址。这就增加了上述第二种追踪方式的风险，即 当设备连接到公共 WiFi 网络或本地蓝牙信标时发生的风险。

2、车辆跟踪和ALPR

自动车牌读取器 ALPRs，是一种配备有检测和读取车牌能力的监视摄像头，它们还可以利用汽车的其他特征，如品牌、型号、颜色和磨损，来帮助识别汽车。

ALPR 通常由警察部门使用，但许多 ALPR 设备由私人公司拥有。这些公司不分青红皂白地收集所有车辆的数据，一旦他们掌握了这些数据，就可以把这些数据再卖给任何人：当地警察、联邦移民执法机构、私人数据聚合商、保险公司、甚至赏金猎人（私家侦探）。

不同的公司从不同的来源收集车牌数据，并将其出售给不同的受众。在美国，数字识别网络（Digital Recognition Network，简称DRN）的数据来源于全国各地数千家收车机构，并将数据出售给保险机构、私人调查员和 “资产回收” 公司。

根据 Motherboard 的调查，被DRN收集数据的绝大多数个人并没有犯罪嫌疑、也没有叫拖车。创业公司 Flock Safety提供由 ALPR 驱动

的“邻里守望”服务（就是群众斗群众），业主可以在自己的物业上安装ALPR，以便记录和分享开车经过自己小区的所有汽车的信息。

DRN 由 VaaS International Holdings 拥有，这是一家位于沃斯堡的公司，该公司将自己标榜为“车牌识别 **(‘LPR’)**和面部识别产品和数据解决方案的卓越供应商”。它还拥有 Vigilant Solutions，另一家ALPR技术的私人传播者。

Vigilant 的客户包括警察机构和私人购物中心。Vigilant 将来自全国各地数千个来源的数据汇集到一个单一的数据库中，它称之为“PlateSearch”。数十家执法机构为访问 PlateSearch 付费。

根据EFF的研究，Vigilant 记录的大约**99.5%**的车牌在被扫描时与公共安全利益完全无关。

摄像头和机器视觉并不是唯一能够实现车辆跟踪的技术。被动式MAC地址跟踪也可用于跟踪车辆运动。车辆内部的电话、有时是车辆本身，都会广播包括其MAC地址在内的探测请求。战略性地放置在道路周围的无线信标可以监听这些信号。一家名为 Libelium 的公司销售一种无线信标，这种信标旨在安装在路灯上，以便跟踪附近的交通。

3、人脸识别监视相机

人脸识别已经在一些国家的执法部门广泛部署，包括中国和英国。这具有可怕的影响：它允许大规模记录无辜者的一举一动。在中国，它不仅被用来监视和控制维吾尔族社区的成员。

媒体报道往往只关注警察部门使用人脸识别相关的公民自由危害。但是，人脸识别也已经被部署在一些私营行业中。比如 航空公司在登机前使用人脸识别来验证乘客的身份；音乐会场馆和票贩子用它来筛选音乐会的观众；零售商使用人脸识别来识别那些据说有较大购物风险的人 …… 私人保安公司出售配备了人脸识别功能的机器人，用于监控公共场所，帮助雇主掌握员工的情况。而学校甚至夏令营也用它来监视孩子们的一举一动。

大型科技公司已经开始投资于面部识别功能的支付处理，这将使他们有另一种方式将现实世界的活动与用户的在线角色联系起来。Facebook 已经申请了一项系统专利，该系统可以将人脸与社交媒体资料联系起来，以便处理支付。另外，亚马逊的实体店 “Go” 也依靠生物识别技术来追踪进入的人和他们拿走的任何东西，以便收取相应的费用。

此外，许多人认为面部识别是将定位广告带入物理世界的一种合理方式。人脸识别相机可以安装在商店、广告牌和商场中，以描述人们的行为，建立每个人的行为习惯档案，并向人们发送定位信息。

2019年1月，Walgreens 开始了一项试点计划，使用安装在冰箱门LED屏幕上的人脸识别相机。这个想法是，消费者不需要透过玻璃板看冰箱里的东西，而是可以看一个屏幕，屏幕上会显示图形，表明里面有什么。监视摄像机对站在冰箱前的人进行面部识别，图形可以动态改变，以提供针对该人的定位广告。无论 Walgreens 最终是否会在更大范围内部署这项技术，这似乎都是零售商的一个方向。

4、支付处理器和金融科技

所谓的”金融科技”，是对与金融相关的技术公司这一新兴行业的总称。数以千计的相对较新的科技公司充当了老牌金融机构和较新技术（包括跟踪和监控技术）之间的粘合剂。这些金融科技公司往往比银行等传统机构受到更少的政府监督。

支付处理商是代表其他企业接受付款的公司。因此，他们掌握了大量有关企业销售和人们购买的信息。由于大多数金融交易都涉及信用卡号码和姓名，支付处理商很容易将他们收集的数据与真实身份联系起来。

其中一些公司是纯粹的服务提供商，除了将钱从一个地方转移到另一个地方之外，不会将数据用于任何其他目的。而另一些则是建立消费者或企业的档案，然后将这些数据货币化。例如，Square 是一家为小企业生产信用卡阅读器的公司，它还利用收集到的信息向第三方提供有针对性的广告，并通过其 Square Capital 计划承保贷款。

一些金融科技公司直接向用户提供金融服务，比如 TurboTax 和 Mint 背后的 Intuit 公司。其他公司则为银行或企业提供服务。

在金融科技领域，“数据聚合商”充当了银行和其他服务之间的中介，比如理财应用。在这一过程中，数据聚合商获得了所有通过其管道的数据，包括数百万人的账户余额、债务和信用卡交易。

此外，聚合商还经常收集消费者的用户名和密码，以便从银行提取数据。Yodlee 是该领域最大的公司之一，它将交易数据出售给对冲基金，而对冲基金则挖掘这些信息，为股市走势提供参照。

许多用户并不知道自己的数据除了用于操作他们注册的应用程序外，还被用于非常多的其他用途。

5、追踪和企业权力

许多从数据跟踪中获益最大的公司都有令人信服的方法来吸引网络开发者、应用创建者和商店经理安装他们的跟踪技术。拥有垄断权力或近乎垄断的公司斗可以利用其市场力量建立跟踪网络，监控和抑制较小的竞争对手，并利用消费者的隐私人权来获得自己的经济优势。

公司权力和公司监控在几个方面相互加强。

首先，谷歌和 Facebook 等最大的寡头公司向出版商施压，要求他们安装跟踪代码。出版商依靠世界上最大的社交网络和世界上最大的搜索引擎来推动自己网站的流量。因此，大多数出版商需要投放广告。而为了追踪他们的广告效果如何，他们别无选择，只能在自己的网站和应用上安装谷歌和 Facebook 的跟踪器。

谷歌、Facebook 和亚马逊也是第三方广告网络，共同控制着超过三分之二的市场。这意味着想要实现内容货币化的任何出版商都很难避开大平台的广告追踪代码。

其次，垂直整合的科技公司可以控制追踪市场的两个方面。谷歌管理

着世界上最大的行为广告系统，它通过收集安卓手机和 Chrome —— 世界上最流行的移动操作系统和最流行的网络浏览器 —— 的数据来提供动力。与同行的操作系统和浏览器相比，谷歌的用户软件使其追踪器更容易收集数据。

当Web设计者第一次描述浏览器时，他们称其为 “用户代理”：代表用户在互联网上采取行动的软件。但是，当一个浏览器制造商同时也是一家以监视资本主义为收入来源的公司时，公司在用户隐私和控制方面的承诺与公司在追踪方面的利益是完全相悖的。利益通常会占上风。

第三，数据不仅可以用来剖析人，还可以用来剖析竞争对手的公司。最大的数据收集者不仅知道每个人的行为方式，他们还比任何人都更了解市场和他们的竞争对手。

谷歌的跟踪工具监控着全网 80% 以上的流量，这意味着它对竞争对手流量的了解往往和竞争对手一样多（甚至更多）。

Facebook (通过第三方广告、分析、转换像素、社交小工具以及臭名昭著的间谍 VPN应用) 也监控着大大小小的网站、应用和出版商的使用和增长情况。亚马逊已经在其 Amazon Web Services 中托管了大面积的互联网，并开始建立自己强大的第三方广告网络。

这些巨头利用这些信息来识别新生的竞争对手，然后在它们成为重大威胁之前将其收购或克隆其产品。根据内部机密文件，Facebook 利用其 VPN Onavo 的用户行为习惯数据，为其收购 WhatsApp 提供信息。

第四，随着科技巨头将追踪权力集中到自己手中，他们可以将获取数据作为反竞争的砝码。也就是数据权力。

Facebook 很清楚，对其API的访问权 (以及由此带来的详细私人数据) 对其他社交公司来说是无价的。**Facebook** 最臭名昭著的历史就包括，允许或拒绝访问用户数据，以破坏竞争。

此外，谷歌和 Facebook 都已经开始采取政策，限制竞争对手对其数据的访问，而不限制他们自己收集的数据。

例如，现在大多数大型平台都限制了自己网站上的第三方追踪器。在谷歌自己的实时出价版本中，谷歌最近开始限制对广告识别器和其他信息的访问，这些信息将允许竞争的广告网络建立用户档案。而在“剑桥分析公司”事件之后，Facebook 开始锁定对第三方API的访问权限，但是并没有对 Facebook 自身收集的用户数据进行任何有意义的改变。

一方面，限制第三方访问可以带来隐私方面的好处。但另一方面，将第三方开发者和外部行为者踢出 **Facebook** 和谷歌的平台服务，只会使垄断问题变得更加严重，让现有巨头对其收集的用户数据独揽大权，并巩固其危害隐私的监视资本主义体制。

与其将竞争和隐私视为孤立的问题，不如赋予用户权力，需要解决这两个问题，以减少大公司对用户数据和注意力的控制。

最后，这些寡头公司可以通过并购获得其他公司的大量数据。Google Analytics 以独立公司 Urchin 起家，Google 在2005年收购了这家公司。2007年，谷歌通过收购 Doubleclick 来超额完成其第三方广告网络，从而成为了现在行为定向广告市场的领导者。2019年底，它又收购了健康数据公司 Fitbit，将每个人多年积累的步数和运动记录合并到谷歌自己庞大的用户身体活动数据库中。

在其短暂的存在中，Facebook 已经收购了67家其他公司。亚马逊收购了91家，谷歌收购了214家 —— 平均每年超过10家。

Facebook、亚马逊或谷歌所收购的许多小公司都能获得大量数据和数百万活跃用户。

每一次收购，这些数据源都会被整合到科技巨头控制的已经非常庞大的数据权力孤岛中。而由于网络效应，当这些数据都放在一个屋檐下时，就会变得更加有价值。

单独来看，Doubleclick 可以组装出用户完全浏览历史的假名资料。但作为谷歌的一部分，它就可以将这些数据与真实姓名、位置、跨设备活动、搜索历史、和社交图谱合并起来，形成有关每个人的详细档案。

那些数十亿美元的科技巨头并不是唯一跟踪您的恶魔。但他们规模越大，知道的东西就越多。而一家公司能够获得的数据种类越多，其对用户和竞争对手的控制权就越强大。

在监视资本主义经济体制中，富人只会越来越富。

[image]

第3部分：定位，代理和实时出价

数据收集后会去哪里？大多数追踪者并不是自己收集每一条信息的。相反，各公司共同合作，为自己收集数据，并相互分享。

有时，拥有同一个人信息的公司只会将其简单地结合起来，以确定哪个广告商将向该人提供哪种广告。在其他情况下，公司将其整个商业模式建立在收集和销售他们从未与之互动的个人数据上。

在所有情况下，他们收集和分享的数据类型都会影响目标用户的体验，无论是通过影响他们接触到的广告，还是通过决定他们最终被编入哪些政府数据库。

此外，用户的数据被传播得越多，受到有害数据泄露影响的风险就越大。本节将探讨个人信息是如何被共享的，以及它的去向。

1、实时出价

实时出价系统是出版商和广告商用来提供目标广告的系统。互联网广

告界的销售单位是“印象”。每当一个人访问一个有广告的网页时，这个人就浏览了一个广告印象。在幕后，广告客户向广告网络支付向您展示广告的权力，广告网络向您看到广告的网页的出版商支付费用。

但是，在这之前，出版商和广告网络必须决定显示哪些广告。为此，他们要进行一场拍卖，拍卖者提供用户的个人信息，然后几十台公司服务器上的软件对该用户的眼球进行竞价。数据流向一个方向，资金流向另一个方向。

这种“实时出价”是相当复杂的，这个主题可以单独编写一份白皮书。幸运的是，关于这个话题已经有了非常多深入的资源。Johnny Ryan 博士和 Brave 写了一系列关于RTB的隐私影响的文章。还有一篇关于协议的隐私影响的博士论文。本节将简要概述这个过程是什么样的，其中大部分是基于 Ryan 的研究工作。

[image]

首先，数据从你的浏览器流向广告网络，也就是“供应方平台”（SSP）。在这种经济中，你的数据和你的眼球（注意力）就是广告网络和**SSP**出售的“供应”。

每个SSP都会收到你的身份信息，通常是以 cookie 的形式，并根据它对你过去行为的了解，生成一个“出价请求”。接下来，SSP将这个出价请求发送给每一个表示有兴趣展示广告的几十家广告商。

[image]

出价请求包含有关您的位置，兴趣和设备的所有信息，并包括您的唯一ID。上面的屏幕截图显示了 OpenRTB 出价请求中包含的信息。

[image]

最后，轮到竞价者了。利用自动化系统，广告商看了你的信息，决定是否要向你做广告，以及要展示哪一个广告，然后向SSP回复出价。SSP决定谁在竞价中获胜，并将获胜者的广告显示在发布者的网页上。

竞价请求中的所有信息都会在任何资金转手之前共享。而没有赢得竞

价的广告商仍然会收到用户的个人信息。这就实现了“影子竞价”。某些公司可能会假装对购买印象感兴趣，但故意在每次拍卖中竞价输掉，目的就是以尽可能便宜的价格收集到尽可能多的数据。

此外，在SSP和广告主之间有多层公司都参与实时出价，每一层公司也都会对用户信息进行吸纳。

SSP与“广告交易所”对接，“广告交易所”与“需求方平台”(DSP)共享数据”，需求方平台也从数据经纪人那里共享和购买数据。发布商与SSP合作销售他们的广告空间，广告商与DSP合作购买广告空间，广告交易所则连接买卖双方……您可以在这里阅读为广告商撰写的SSP和DSP之间的差异分析。

很难理解也没关系，您只需要知道：参与整个过程的每个人都能收集到您的行为数据。

在竞价过程中，广告商和与之合作的DSP可以使用第三方数据经纪人来增强他们掌握的个人用户的资料。这些数据经纪人自称为“数据管理平台”(DMP)，他们根据竞价请求中包含的身份标识和人口统计数据出售个人数据。换言，广告商与数据经纪人共享用户ID，并获得该用户的行为档案作为回报。

[image]

上图再次展示了单个实时出价拍卖中的信息和资金流向。

从访问页面的用户的角度来看，实时出价造成了两组独立的隐私侵犯。

首先，在人们访问页面之前，一系列公司跟踪你的个人信息，包括在线和离线，并将其合并成一个关于您的复杂的档案。然后，在实时出价过程中，一组不同的公司使用该档案来决定广告印象的出价。

作为用户访问页面的结果，实时出价参与者从访问用户那里收获了额外的信息。这些信息被注入到用户的旧档案中，以便在其下一次访问页面所触发的后续实时出价中使用。

因此，实时出价既是追踪的原因，也是追踪的手段。

网络上的实时出价工具：**Cookie**同步

Cookie同步是网络追踪者用来将 Cookie 相互链接、并将一家公司拥有的关于用户的数据与其他公司可能拥有的数据相结合的一种方法。

从机制上讲，它非常简单。一个跟踪域触发对另一个跟踪器的请求。在请求中，第一个跟踪器发送一份自己的跟踪 cookie 的副本。第二个跟踪器同时获得自己的 cookie 和第一个跟踪器的 cookie。这样，它就可以与另一个跟踪器进行 “比较说明”，同时建立起它对用户的档案。

Cookie共享通常作为实时出价的一部分被使用。在竞价请求中，SSP 与所有潜在投标人共享自己的 CookieID。在没同步的情况下，需求方平台可能会有自己的关于用户的档案与自己的cookieID挂钩。

一个DSP可能不知道 Doubleclick（谷歌的广告网络）的用户 “abc” 和自己的用户 “xyz” 是同一个人。而Cookie 同步就让他们能够确定这点。

作为竞价过程的一部分，SSP通常会同时向许多DSP触发 Cookie 同步请求。这样一来，在SSP下次发出出价请求时，将要出价的DSP可以使用他们自己的关于用户的行为档案来决定如何出价。

[image]

移动应用中的实时出价

实时出价是为Web创建的，但它同样适用于移动应用中的广告。追踪者使用广告ID来代替 cookies。

iOS和安卓系统中内置的广告ID让追踪者的工作更加轻松。在网络

上，每个广告主都有自己的 cookie ID，需求方平台需要与 DMPs 以及彼此同步数据，以便将他们的数据与特定用户绑定。

但在移动设备上，每个用户都有一个通用的广告ID，每个应用都可以访问。这意味着，上述描述的在web上的同步程序在移动设备上没有必要，广告商可以使用广告ID来确认身份，共享数据，并建立更详细的档案，在此基础上出价。

2、群体定位和相似受众

有时，大型平台并不披露他们的数据，而是临时出租其数据驱动的工具的访问权。Facebook、谷歌和 Twitter 都允许广告商针对各类人群投放广告。例如，Facebook 允许广告商针对具有某些 “兴趣” 或 “亲和力” 的用户。

这些公司不会向广告商展示其活动目标个人的实际身份。如果你在 Facebook 上发起一个活动，目标是 “对圣地亚哥轮滑阻拦赛兴趣的人”，你无法马上看到一个名单。然而，这种定位确实允许广告商直接接触到参加比赛的圣地亚哥人，并将他们引导到外部网站或应用程序。

当目标用户点击广告时，他们会被引导离开 Facebook，进入广告商的域名。此时，广告商知道这些人来自 Facebook，并且他们是目标人群的一部分。一旦用户登陆第三方网站，广告商就可以利用数据交换服务将他们与行为特征甚至现实世界的身份进行匹配。

此外，Facebook 还允许广告商根据其他人群建立 “外观相似的受众”。例如，假设你是一家有网站的发薪日贷款公司。你可以在你的债务人访问的页面上安装一个隐形的 Facebook 追踪像素，列出访问该页面的人的名单，然后要求 Facebook 创建一个 “look-alike” 受众，这些人是 Facebook 认为与您的名单上的人 “相似” 的人。

然后，您就可以在 Facebook 上针对这些人投放广告，引导他们回到你的网站，在那里你可以使用 cookies 和数据交换来识别他们是谁。

这些 “look-alike” 的功能完全是黑盒子。如果不能对它们进行审计或研究，就不可能知道它们使用了什么样的数据，以及它们可能会暴露出什么么样的用户信息。

3、数据经纪人

数据经纪人是收集、汇总、处理和销售数据的公司。他们在普通用户看不见的地方经营，但的确处于数据共享经济的中心。

通常情况下，数据经纪人与用户根本没有直接关系，他们出售数据的对象可能完全不知道他们的存在。

数据经纪人从各种小公司购买信息，包括零售商、金融科技公司、医疗研究公司、在线广告商、手机供应商、物联网设备制造商、还包括地方政府。

然后，他们将数据或数据驱动的服务出售给广告商、房地产商、市场研究公司、高校、政府、私家侦探赏金猎人、和其他数据经纪人。

这又是一个太过宽泛的话题，在此不做赘述，其他人已经对数据销售生态系统进行了深入的分析。Cracked Labs 关于企业监控的报告既方便又深入。世界隐私论坛的 Pam Dixon 也对数据经纪人做了很好的研究，包括2014年的报告以及2015年和2019年在参议院的证词。

“数据经纪人” 这个词的含义非常广。它包括组装和销售电话号码或电子邮件列表的营销小公司，也包括像甲骨文这样的庞然大物，它们从成千上万的不同流中摄取数据，并向其他企业提供基于数据的服务。

一些经纪人出售原始信息流。这包括有关零售购买行为的数据、来自物联网设备的数据、以及来自联网汽车的数据。

另一些则充当各种数据的买家和卖家之间的信息交换所。例如，Narrative 承诺帮助卖家 “释放[他们]数据的价值”，并帮助买家 “访问

[他们]需要的数据”。Dawex 将自己描述为“一个全球数据市场，在这里你可以直接面见、出售和购买数据”。

另一类公司充当中间人或“聚合器”，从多个不同来源获得原始数据的许可，对其进行处理，并将其重新包装为其他企业的特定服务。

例如，主要的手机运营商将位置数据的访问权卖给了名为 Zumigo 和 Microbilt 的聚合商，而后者又将访问权卖给了其他一系列广泛的公司，由此产生的市场最终达到了保释担保人和赏金猎人的手里（以及一名卧底记者）。

许多最大的数据经纪人并不出售他们收集到的原始数据。相反，他们从数以千计的不同来源收集和消费数据，然后利用这些数据组建自己的档案，并对个人进行推断。

全球最大的数据经纪人之一甲骨文公司拥有网络上最大的第三方追踪器之一 Bluekai。包括 Equifax 和 Experian 在内的信用报告机构在这里也特别活跃 —— 就是负责信用评分的机构。

虽然美国《公平信用报告法》规定了信用评分机构如何分享特定类型的数据，但是，并不妨碍这些信用机构出售追踪者收集到的大部分信息，包括交易信息和浏览历史记录。

这些公司中的许多公司都在宣传他们能够推导出心理特征，即 描述用户行为的“天生”特征。

剑桥分析公司（Cambridge Analytica）臭名昭著，它利用有关 Facebook 点赞的数据，得出了数百万选民的“OCEAN评分” —— 开放性、认真性、外向性、合意性、甚至神经质程度的评分，然后用这些数据卖给政治活动以操纵选举。

最后，许多经纪人利用他们的内部资料向他人提供“身份解析”或“充实”服务。如果一个企业拥有一个身份标识，如 cookie 或电子邮件地址，它就可以向数据经纪人支付费用，以“充实”该数据并了解该人的其他信息。它还可以将与一个标识符（如cookie）绑定的数据与另

一个标识符（如移动广告ID）的数据联系起来。

在实时出价领域，这些服务被称为“数据管理平台”。实时竞价者可以利用这类服务来了解某个用户是谁，他们的兴趣是什么，只需根据竞价请求中包含的ID即可。

数据使用者

到目前为止，本文已经讨论了如何收集，共享和出售数据。但是，最终结果在哪里？谁是个人数据的使用者，他们将如何处理？

1、定向广告

到目前为止，最大、最明显、最无处不在的数据使用者是定向广告商。定向广告允许广告商根据人口统计学、心理学和其他特征来接触用户。行为广告是定向广告的一个子集，利用用户过去的行为数据来进行个性化的广告。

最大的数据收集者也是最大的定向广告商。谷歌和 Facebook 共同控制了美国近60%的数字广告市场，他们利用各自的数据库来实现这一目标。

谷歌、Facebook、亚马逊和 Twitter 提供点到点的定向服务，广告商可以针对高级别的用户进行定向，而广告商本身不需要获取任何数据。

Facebook 让广告商根据位置、年龄、性别、教育和收入等人口统计学数据；以及爱好、音乐类型、名人和政治倾向等兴趣数据来定位用户。

Facebook 使用的“兴趣”有些是基于用户“点赞”或评论的内容，有些则是基于 Facebook 的第三方追踪而得出的。虽然 Facebook 利用其数据为广告商匹配目标受众，但 Facebook 并不与这些广告商分享

其数据。

实时出价（RTB）涉及到更多的数据共享，有大量的小公司参与到这个过程的不同层面。大的科技公司也在这个领域提供服务。谷歌的 Doubleclick Bid Manager 和亚马逊DSP都是RTB需求方平台。

在实时出价中，身份标识是共享的，这样广告主自己（或他们的代理商）就可以决定是否要接触到每个人，以及他们要展示什么广告。

在RTB生态系统中，广告商收集自己的用户行为数据，他们可能会使用内部的机器学习模型来预测哪些用户最有可能参与他们的广告或购买他们的产品。

一些广告商想在 Facebook 或谷歌上接触用户，但又不想使用大公司的专有定向技术。相反，他们可以从数据经纪人那里购买联系人信息列表，然后将这些列表直接上传到 Facebook 或谷歌，后者将在其所有平台上接触这些用户。

这个系统破坏了大公司控制歧视性或其他恶意目标的努力。谷歌和 Facebook 等定向平台不允许广告商针对特定种族的用户发布工作、住房或信贷广告。

但是，广告商可以从数据经纪人那里购买个人的人口统计信息，上传一份恰好来自同一种族群体的名单，让平台直接针对这些人。谷歌和 Facebook 都禁止使用 “敏感信息” 来锁定联系人名单上的人，但目前还不清楚他们如何执行这些政策。

2、政治运动和利益集团

公司并不是唯一试图从数据收集和定向广告中获益的实体。剑桥分析公司就是个最著名的例子，它们使用不正当得来的个人数据以估计数百万潜在选民的 “心理特征”，然后使用这些数据来操纵政治。

2018年，CatholicVote 组织利用手机位置数据确定谁曾进入过天主教

堂，然后针对他们发布竞选广告。反堕胎组织使用类似的地理围栏技术，在妇女去堕胎诊所时向她们定向投放广告。

而这些事件并非孤立。一些依靠捐款的非营利组织购买数据，帮助缩小潜在捐助者的范围。许多政客都利用公开的选民登记数据来锁定选民。据报道，民主党全国委员会正在2020年大选前大力投资其“数据仓库”。而共和党的咨询公司 Deep Root Analytics 是美国史上最大的选民数据泄露事件的源头，该公司一直在收集近2亿美国人的姓名、登记细节以及“模型化”的种族和宗教数据。

3、讨债者、赏金猎人和欺诈调查员

讨债者、赏金猎人和调查机构都从一些来源购买和使用位置数据。EFF正在起诉 AT&T，因为它将位置数据出售给聚合商，使赏金猎人能够进入二级市场。

然而，手机运营商并不是该数据的唯一来源。保释金公司 Captira 将从手机和车牌阅读器收集的位置数据出售给赏金猎人，价格仅为7.5美元。

而数以千计的应用程序利用GPS权限收集位置数据，然后将这些数据卖给下游的聚合商。这些数据可以用来定位任何人。而且正如调查所显示的那样，它也可以被几乎任何人购买和滥用。

4、城市、警察部门和间谍机构

公共部门也从私营部门购买数据，用于各种用途。例如，美国移民和海关执法局从 Vigilant 公司购买了ALPR数据，以帮助定位该机构驱逐移民。

加利福尼亚城市联盟（League of California Cities）在一封信中称，政府机构与数据经纪人签订合同，以完成无数任务，从确定人类服务的资格到收税，寻求该州消费者数据隐私法对政府机构和数据经纪人之间合同的例外。

长期以来，倡导者一直谴责政府机构和私人数据经纪人之间的这些安排，谴责其是对消费者数据隐私的威胁，也是对政府自身数据库法律限制的终结。

当然，所谓的国家安全监控往往是建立在对私营公司的消费者数据库进行数据挖掘的基础上。例如，作为爱德华·斯诺登披露的 **PRISM**（棱镜）计划的一部分，**NSA** 直接从谷歌、**YouTube**、**Facebook** 和雅虎收集个人数据。

[image]

第4部分：反击

不幸的现实是，跟踪是难以避免的。数千名独立的监视者使用数百种不同的技术，企业监控是广泛的，而且资金充足。虽然没有任何一键式的东西可以阻止每一种追踪方法，但您仍然可以做很多事来夺回您的隐私。

每个人都应该自己决定愿意为保护自己的人权和安全付出多少努力。小的改变就可以明显减少追踪者可以收集和分享的数据量，比如在浏览器中安装 Privacy Badger，以及更改手机上的设置。

更大的改变，比如卸载第三方应用和使用 Tor，可以提供更强的隐私保证。对于那些有严重顾虑的用户来说，更强的措施可能是值得的。

请记住，这一切都不是你的错。隐私不应该是个人责任的问题。这不是您的工作，您不应该去读那些25万字的隐私政策中莫名其妙的法律术语才能了解您的手机如何共享数据。隐私应该是一种基本人权，而不是受过良好教育和有闲暇时间的人的特权。每个人都应该生活在一个尊重自己隐私的世界里，无论是在线还是离线。

在手机上

阻止移动设备上的跟踪器是比较复杂的。没有一种解决方案，比如浏览器或扩展，可以覆盖很多基础。而且不幸的是，在某些设备上根本无法控制某些种类的跟踪。

抵御追踪的第一道防线是您的设备设置。

[image]

iOS 和 Android 都可以让用户查看和控制每个应用所拥有的权限。您应该检查所有应用所拥有的权限，并删除不需要的权限。

您可以简单地删除您不使用的应用程序。除了每个应用程序的设置外，您还可以更改全局设置，这些设置会影响您的设备如何收集和共享特别敏感的信息，如位置。您还可以控制应用程序在不使用时如何允许其访问互联网，这可以防止被动跟踪。

这两种操作系统可以选择以不同的方式重置设备的广告ID。在iOS系统中，可以通过将广告ID设置为一串零来完全删除它。在Android上，您可以手动重置它。这相当于清除 cookie，但不会阻止新的 cookie：它不会完全禁用跟踪，但会使跟踪者更难建立关于您的统一档案。

安卓系统还有一个 “退出基于兴趣的广告” 的设置。这向应用程序发出了一个信号，即 用户不希望自己的数据被用于定向广告，但实际上并没有通过广告ID来阻止应用程序这样做。事实上，最近的研究发现，数以万计的应用根本无视这个信号。

在iOS上，有少数应用可以过滤其他应用的追踪活动,在 Android 上就没那么容易了。谷歌在其应用商店 Play Store 中禁止广告和追踪器拦截器，所以它没有官方审核的这类应用。可以从 Play Store 之外 “侧载” 拦截器，但这可能非常危险。确保你只安装来自你信任的发行商的应用，最好是开源的。

您还应该考虑您的设备正在与之通信的网络。最好避免连接到不熟悉的公共WiFi网络。

无线信标也在试图收集您的设备的信息。只有当您的设备正在广播其硬件MAC地址时，它们才能收集识别信息。现在 iOS 和 Android 都会默认随机化这些MAC地址，但其他种类的设备可能不会。

您的电子阅读器、智能手表或汽车都会广播探针请求，追踪者可以利用这些请求来获取位置数据。为了防止这种情况发生，您通常可以关闭WiFi和蓝牙，或者将设备设置为 “飞机模式”。这也是一个省电的好方法。

最后，如果您的确需要匿名，使用一次性手机可以帮助您控制与固有硬件标识符相关的跟踪。

现实中

首先您应该了解，如今在现实中您已经基本无法离线了。没有选择 “退出” 的按钮。

如上所述，有许多方法可以修改您的设备工作方式，以防止它们对您不利。但是，要避免人脸识别摄像头和自动车牌阅读器的追踪几乎是不可能的。

当然，我们介绍过一些混淆人脸识别算法的思考方式，您也可以选择不买车来远离ALPR监视数据库，您可以使用现金或虚拟信用卡来阻止支付处理器对您进行追踪描述。

但期待完全摆脱监视在当前世界是不现实的，所以非常建议您将工作和生活分层处理，每一层根据其不同的敏感等级采取不同的和恰当的保护性措施。

[image]
[image]

互联网作为新的圈地运动

[image]	关键词	元宇宙 操纵 监视资本主义 算法暴政 认知 高堡奇人
[image]	关联	；[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？ ；👁🗨大规模数字监控
[image]	创建时间	2021年11月11日
[image]	**Description**	技术直觉

这就是我们继承的那种互联网：一个垄断性的数字购物中心，而不是一个公社。而它所帮助产生的社会只是类似于《雪崩》，而不是《星际迷航》。

- Table of Contents
妖魔鬼怪的社会
“头号世界”
元宇宙的秘密
互联网作为新的圈地运动
数字化资本主义、注意力经济和监视国家

[image]

上图不是玩笑。

关于美国和中国在人工智能领域争夺主导地位大权的技术军备竞赛，一直存在着激烈的辩论。但现在最具有战略意义的问题是：中国是否正在建设元宇宙。

在人工智能等基础设施技术的基础上，元宇宙指的是大量的数字体验和生态系统，从电子商务和娱乐到社交媒体和工作，人们在这里度过越来越多的生活 —— 换句话说，趋向一个无人能离线的世界。很可能很快，整个社会和经济生活中的大部分内容都是由元宇宙的规则来定义的。谁在建立这个世界，谁就是这个世界的独裁者。

美国和中国都在试图建立并宣称拥有元宇宙，欧洲等其他行为体也在试图这样做，但后者根本没有控制足够的核心技术，只有这些技术能使元宇宙成为可能。

换句话说，只有高堡奇人能做到，而且正在做。这就是为什么中国公民和美国公民对元宇宙的危险性的了解，具有最大的意义 —— 只有你们才能阻止这一灾难，在为时已晚之前。

[image] 中国巨头腾讯已经开始分享其“元宇宙”愿景

创始人马克·扎克伯格却梦想着不向外太空而是向网络空间扩张。硅谷的领主们都已经完成了地球上的现实，但是当埃隆·马斯克和杰夫·贝索斯安排计划实际离开的时候，扎克伯格想要设计一个更好的地球体验——
一个由 Facebook 策划的体验。 [image] 当其他的科技CEO们试图开创一个大规模星际旅行的时代时，Facebook

今年7月，扎克伯格宣布，Facebook 正在向一个 “元宇宙” 公司转型，在未来五年内。这个社交媒体巨头希望蜕变为一个无所不包的平台，将社交关系、工作、商业和娱乐融合在一个大帐篷下。

如果您觉得这很模糊，那是因为所谓的元宇宙是一只章鱼，几乎有无限的手臂，没有单一的蓝图，这就是为什么许多人称它为**Web 3.0**。它是 “移动互联网的继任者”，扎克伯格上个月告诉 Verge：“你可以把元宇宙看作是一个具体的互联网，在这里，你不仅仅是在观看内容，而是身在其中”。

作为他最初的元宇宙媒体闪电战的一部分，上个月出现在CBS新闻上使用 Horizon Workrooms 展示了 “在互联网中” 的实际含义。

Workrooms 是 Facebook 试图超越 Zoom 的产品，是一个沉浸式的电

话会议程序，同事们戴上 Oculus VR 头盔，共享一个虚拟的办公空间，比如，用手势在数字白板上涂鸦，而他们的数字化身则模仿他们自己的动作。这个演示看起来令人啼笑皆非（那些卡通化的化身看起来就像任天堂做了一个叫 Wii Work 的应用程序后的样子），但很容易理解为什么管理层会对一个看起来温和的、色彩鲜艳的全景式工作场所趋之若鹜 —— 因为在那里，即使在你自己的卧室也不可能逃脱你老板的目光了。

根据扎克伯格的说法，Horizon Workrooms 只是未来的一个尝试。他说："五年后，人们将能够住在他们想住的任何地方，在他们想工作的任何地方工作，并具有存在感"。

如果元宇宙的想法超越了通过 Oculus 头盔的护目镜所看到的愚蠢的CGI驱动的技巧，那么 "存在"
的定义可能会在未来几年内完全被改变（尽管扎克伯格的半个月时间表似乎很乐观）。许多元宇宙的设计者设想了这样一个未来：物理、增强现实和虚拟现实融合成一个单一的 "现实"，由一个共享的经济和媒体消费系统管理。

风险投资家马修·鲍尔 (Matthew Ball) 去年1月在一篇有影响力的文章中概述了元宇宙的概念。他写道，元宇宙 "不仅将彻底改变数字世界的基础设施层，而且还将彻底改变大部分物理世界，以及在其之上的所有服务和平台，它们如何工作，以及它们销售什么"。换句话说，元宇宙将创造一个全新的消费品所有权领域。

例如，想象一下，你为自己在视频游戏《堡垒之夜》中的数字头像购买一个《瑞克与莫蒂》主题的皮肤。目前这是有可能的，但只能通过购买1500个《堡垒之夜》的游戏币V-Bucks。装扮成瑞克·桑切斯(Rick Sanchez)只在流行的大逃杀射击游戏中有效。理论上，元宇宙基础设施将使你能够转移数字装备，在 Lady Gaga 的在线音乐会中（计划明年在《堡垒之夜》中使用）或与朋友一起进行 Peloton 团体锻炼时穿着它。

> "如果元宇宙让你听起来就像是从某本科幻小说上撕下来的书页，那是因为它确实如此。"

假设你的恶作剧做得太过火了，老板很恼火，因为你以卡通科学家的身份出现在现实生活中的会议上，每个人都通过他们的雷朋智能眼镜看到了这一点。然后，你羞涩地决定用这套服装换取货币，形式是“酷猫”不可伪造代币（NFT）和一把狗狗币。也可能发生了相反的情况，你非常喜欢它，你不仅想永远保留瑞克的皮肤，还想把它写进你的遗嘱，在你死后把它传给你的孩子。所有这些，甚至更多，都可以在元宇宙中实现。

如果元宇宙让你听起来就像是从某本科幻小说上撕下来的书页，那是因为它确实如此。

[image]

妖魔鬼怪的社会

元宇宙一词首次出现在尼尔·斯蒂芬森1992年的科幻小说《雪崩》中，该书讲述了阿弘（Hiro）的未来主义冒险，他是给黑手党送披萨的外卖司机，兼职当黑客，沉浸在被描述为“计算机生成的宇宙中。他的计算机正在将其绘制在护目镜上，并将其输入耳机”。

这本书长期以来一直是高科技祭司的圣经。斯蒂芬森被尊称为预言家，除了元宇宙之外，他还发明了虚拟化身和加密货币的概念。《雪崩》曾经是 Facebook 管理团队的必读书。斯蒂芬森与贝索斯结识，并在2014年被增强现实公司 Magic Leap 聘用，帮助实际建立元宇宙。

显然，硅谷的人都没有体会到讽刺感。《雪崩》是一部反乌托邦小说，而不是一部乌托邦小说。

与《黑客帝国》电影或小说《头号玩家》（Ready Player One）等流行文化产品所激发的游乐场般的炼狱相比，《雪崩》中的数字王国甚至更加阴险。吞下《黑客帝国》中的红色药丸意味着刺破幻觉的面纱，体验到一个真实的世界。同样，《头号玩家》中的OASIS就像插入了世界上最先进的PlayStation，你可以轻易离开。

在《雪崩》中，一些用户可以登录和退出终端，但 “妖怪”，一类始终佩戴着现实增强设备的角色，从来没有真正做到。对于一直居住在元宇宙中的妖怪来说，不存在 “登录”和 “退出”。

斯蒂芬森写道：

> 他们在一个激光绘制的世界中漂泊，在各个方向上扫描，对一千码内的每个人进行背景调查，同时看到视觉光、红外线、毫米波雷达和超声波中的一切。

通过做出真正的设计来迎接元宇宙，硅谷正试图把我们都变成妖怪。

法国哲学家让·鲍德里亚（Jean Baudrillard）对这种情况有一个说法：超现实，现实和模拟是如此无缝地融合在一起，以至于世界之间没有明确的区别。他推测，最终，这种区别已经不重要了，因为无论如何，人们会从模拟世界中获得更多的意义和价值。

[image]

如果元宇宙无法与现实生活分开，那么元宇宙就是现实生活，以至于 “元宇宙” 这个词本身最终被淡化，建构的现实也变得不可见。考虑一下资本主义是如何成为类似于西方版本的 **Windows** 的东西，一个在新自由主义时代悄然运行的操作系统。现实的终结可能成为新的 “历史的终结”。

你能想象那些拉开这个新现实的弓弦的人的力量吗？扎克伯格可以。

[image] [image]

“头号世界”

有些人认为元宇宙只不过是个空谈。在扎克伯格宣布这一消息后，包括左派在内的一些批评者将其斥为 “数字骗局” 或 “哄孩子” 的骗局，正如 Gawker 讥讽的那样。

一代人之前，许多婴儿潮一代和年轻的X一代对原始互联网到来的消息嗤之以鼻，或者嘲笑它将永远改变社会的想法。我个人知道这一点，因为在1994年冬天，我为我的高中报纸写了一个专题，标题是："什么是互联网？" 它赢得了很多困惑的目光。但后来发生了一件有趣的事。书呆子们赢了，互联网确实改变了一切。

证明 Web 3.0 即将到来的证据无处不在。在过去的二十年里，我们越来越多地放弃了共享的物理和公共空间 —— 鲍德里亚所说的 "真实的沙漠"—— 而去追求超现实的狂喜和通过屏幕进行的体验。有没有想过为什么我们现在需要 "生活" 这个词作为修饰语放在 "体验" 之前？

当《名利场》问斯蒂芬森关于他的小说对当前时代的预测时，他说："现在蜷缩在你手中的长方形（手机）上四处游走的做法是完全正常的，当我看到有人在汽车里或在数百英尺外的街上行走时，我就可以从他们的姿势看出他们在发短信"。

COVID-19的大流行政策，如隔离和社会疏远，使这个世界向数字优先的社会的转变进入了超速状态。在封锁期间，数字设备的平均使用时间每天增加了5小时，重度用户每天粘在设备上的时间约为17.5小时。Zoom 现在有3亿用户，而在2019年12月只有1000万。谷歌、**Facebook**、苹果和亚马逊 —— 信息经济的四大巨头 —— 现在 "大而不倒"，就像美国的顶级银行和制造商在上世纪末那样。

甚至许多抗议团体（不论是极右翼还是左翼），都有一种超现实的质感，仿佛他们从互联网的边缘角落走出来，走到大街上，就像装扮好的网络化身活了过来。由 **Reddit** 驱动的米姆股票、加密货币和**NFT** 的激增，暗示我们的经济也在朝这个方向发展，伊隆·马斯克能够通过一条推文创造财富、也可以摧毁财富。在一个非常现实的意义上，数字工作、游戏、购物、社交和政治，已经在取代而不是补充它们在物理世界的对应物。

视频游戏已经有了类似于元宇宙的品质。2020年，说唱明星Travis Scott 在《堡垒之夜》中举办了五场虚拟音乐会，Epic Games 声称有2770万玩家参加。每天大约有150万人玩 Axie Infinity，在这个游戏中，用户花费数百美元在他们的电脑上饲养类似神奇宝贝的生物，希望能培育出一种罕见的类型，从而获得高额的加密货币。有相当数量

的年轻人退出了正规经济领域，整天养殖 Axies。用 Twitter 的话说就是：打工经济已经疲惫不堪；休闲经济则是有线的。

硅谷认为元宇宙的基础已经到位，也许有充分的理由。鲍尔写道："像这样的根本性变化" 总是一个数十年的迭代过程，"然而，尽管如此，在过去的几年里，有一种明确无误的感觉，即 基础部分正在以一种感觉非常新、非常不同的方式组合起来"。

元宇宙的秘密

像贝索斯、马斯克和扎克伯格这样的硅谷巨头认为，他们最终是人类的大救星，而不是恶棍。他们是吉恩·罗登贝里(Gene Roddenberry)原作《星际迷航》(Star Trek)的粉丝，这部电视科幻作品将太空设想为一张改进社会的空白画布，赞成探索而非殖民主义，外交而非战争，商业而非贪婪。

贝索斯和马斯克还没有大胆到要实现太空社会主义的程度。他们似乎已经接受了一个严峻的事实，即地球正在消亡，因此，人类需要一个逃生舱，进入一个勇敢的新世界，在同样的自由市场资本主义下运作，只是更强调 "自由" 的部分。

但是，虽然从远处看，太空是迷人的研究，而作为一个生活、呼吸和繁荣的地方，嗯，它很糟糕。也许这就是为什么马克·扎克伯格选择不参与这场特殊的太空竞赛，而专注于元宇宙。毕竟 **Facebook** 自己的历史证明，殖民地球人的思想要比殖民火星容易得多。

扎克伯格自己的技术乌托邦主义品牌并不新鲜。它是对**60**年代后网络预言家意识形态的重启，他们将万维网视为新时代自由主义和解放的潜在冥界，一个几乎是精神的旅程，"将使我们摆脱边界和法律，打破身体和心灵的枷锁"。但他的版本恰恰相反，他是在冲淡这一理想。

"我相信，当更多人可以分享他们的经验时，当政府和媒体公司等传统守门人不控制哪些想法可以被表达时，世界会更美好"，扎克伯格

在2019年说。请注意，他说的是个人自由表达，而不是资本、劳动，甚至不是民主。这就是我们继承的那种互联网：一个垄断性的数字购物中心，而不是一个公社。而它所帮助产生的社会只是类似于《雪崩》，而不是《星际迷航》。

仔细阅读斯蒂芬森小说的读者会知道这是一个悲剧。在《雪崩》的黯淡宇宙中，政府已经退居二线，土地被分割成由大企业统治的特许经营的城市国家。无政府的资本主义的胜利反过来又导致了不平等的飙升和物质条件的恶化，而元宇宙为大众提供了一个避难所—— 或者至少是一个转移注意力的地方 —— 来逃避他们周围的堕落社会。

[image]

互联网作为新的圈地运动

许多人将互联网视为创造新公地的机会，即 可以共享而非私人拥有的资源。但是，面对国家和企业对我们每个人在线互动的结构越来越大的权力，我们不得不考虑一种更加根本性的原因，即 互联网代表了一种新的公共资源的封闭性：将通信引导到可以被映射、巡逻和控制的格式。

向资本主义过渡的基础性事件之一是最初的公地圈地运动，即 曾经被所有者自由使用的土地被没收并变成了私有财产。事实上，在整个资本主义的发展过程中，这一圈地运动一再被重复。

似乎很有可能，在 “公地” 受到圈地威胁之前，我们无法认识到这件事。没有人认为 “祝你生日快乐” 这首歌是公有财产，因为声称拥有版权的时代华纳公司没有成功地从其在生日聚会上的表演中获利；农民和原住民最初也不认为土地是共同拥有的财产—— 相反，他们认为土地可以成为财产的想法很荒谬。

仅仅在几代人之前，同样很难想象有一天人们在一起聊天时可以看到相应的广告，你也很难想象你都不知道是谁的人可以一目了然地描绘你的私人品味和社会关系，或者通过监测你的谷歌搜索实时跟踪你的内心活动。

[image]

与其说互联网是“不可避免的自由进步的前沿阵地”，不如说它是与那些不仅要将土地私有化，而且要支配我们每个人的自我身份的每一个方面的统治阶级进行的一场长达几个世纪的竞赛中的最新战场。那些希望捍卫它的人有责任证明它仍然提供了一个自由的疆界。

在这场斗争的过程中，可能会发现，数字自由像所有有意义的自由形式一样，与资本主义和国家无法兼容。

[image]

> 这个媒介将人的经验、记忆和交流转化为合成和外部的东西。在一个媒体驱动的社会中，人们依赖技术来获取自身的这些外在方面。书籍、录音、电影、广播、电视、互联网、手机：这些连续的创新都深入到了每个人的日常生活中，在我们的经验中占比越来越大。

数字化资本主义、注意力经济和监视国家

直到20世纪末，大众传媒基本上还是单向的，信息流向一方，注意力流向另一方。批评者普遍关注其结构的这一方面，指责它给了一小撮人对社会的巨大影响，而使其他人成为旁观者。相比之下，地下媒体则倡导更多的参与性和分散化的形式。

随着可广泛使用的数字媒体的到来，参与和分权突然成为了主流。在许多方面，互联网为新的交流模式提供了一个解放和授权的场所。由于基本模式是由军方资助的研究人员开发的，而不是由私营部门开发的，所以它被设计成有用的而不是有利可图的东西。

- 在这里看到具体解释《 互联网究竟是什么？—— 来自“监视谷”惊人的启示 》

[image]

延伸：https://iyouport.substack.com/p/--d23

直到今天，互联网的大部分仍然是一种狂野西部，在那里很难执行传统的财产法。用户之间自由和直接分享内容的能力对一些行业产生了巨大的影响，而维基百科和开源软件等协作形式表明，人们可以在没有私有财产的情况下轻松满足自己的需求。企业仍在争先恐后地想办法在互联网上赚取网店和广告以外的钱。

[image]

然而，随着我们的生活越来越多地被数字化，重要的是不要想当然地认为这总是最好的结果。资本主义通过吸收世界上曾经是免费的方面，然后以价格提供访问它们的机会而繁荣起来，这种价格并不总是以金钱计算的。

您应该特别注意新媒体的所谓便利方式：这种便利更像是人类生活的无限可能性被强行缩小的标志。事实上，这些创新甚至几乎是可有可无的：而如今，如果你没有手机和网上资料，就很难维持友谊或被雇用。我们越来越多的心理过程和社会生活必须通过技术的调解，这些技术为企业和政府间谍机构绘制我们每个人的一举一动和社交关系。这些格式也塑造了这些活动和关系的内容。

[image]

延伸：https://iyouport.substack.com/p/60d?utm_source=publication-search

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

Facebook 提供的网络并不新鲜；新鲜的是它们似乎对我们来说是外部的。我们一直都有社交网络，但没有人可以利用它们来卖广告 —— 它们也不那么容易被映射。而现在，它们作为我们必须咨询的东西重新出现。早在电子邮件、谷歌和推特之前，人们就与老朋友通信，自学技能，并传播公共事件。当然，这些技术在一个我们很少与邻居

亲近或很少在任何地方呆上几年的世界中是非常有用的。技术和日常生活所承担的形式相互影响，使人们越来越无法想象将它们分开后的结果。

随着人们对信息的需求和获取的增加，超出了可以内化的范围，信息似乎变得与人们分离了。这与将工人转变为消费者的劳动产品强行分离的做法有相似之处，令人怀疑。互联网上的信息并不是免费的——计算机和互联网接入要花钱，更不用说生产这些信息和在世界各地运行服务器的电力和环境成本了。如果企业想出办法，在人你完全依赖这些技术的时候向你收取更多的费用呢？如果他们能做到，不仅是权力和知识，甚至是维持社会关系的能力都将直接取决于财富。

[image]

返回：https://iyouport.substack.com/p/--627?utm_source=publication-search

但这可能是需要注意的错误。旧的财团可能终究无法在这块新的土地上巩固权力。资本主义通过数字技术对我们的生活进行殖民化的方式可能与旧的殖民化形式不一样。

像任何金字塔计划一样，资本主义必须不断扩张，吸收新的资源和主体。它已经延伸到了整个地球；最后的殖民化战争正在喜马拉雅山脚下，即世界的最边缘进行。从理论上讲，它现在应该即将崩溃，因为它已经用尽了视野。但是，如果它可以继续向我们这些人类扩张，而这些新技术就像哥伦布的航船降落在所有人的心理过程和社会关系的大陆上呢？

[image]

在这种说法中，互联网的功能是建立在物质经济上的另一个连续的异化层。如果互联网上的大量内容都是免费的，这不仅仅是因为殖民化的过程还没有完成，而且还因为媒体的决定性货币不是美元，而是注意力。注意力在信息经济中的作用与物质资源的控制在工业经济中的作用相同。即使注意力不能立即转化为网上的收入，它也能帮助确保网上的收入。作为货币，注意力和资本的行为是不同的，但它们都有助于创造权力的不平衡。

资本到底是什么？一旦你剥去那些使它看起来像自然力量的迷信，就能看到，它本质上是一种社会结构，是使一些人能够积累的对他人的权力。如果没有私有财产的概念，而事实上的私有财产只有在每个人都尊重它的情况下才是“真实的”，物质资源就不能作为资本发挥作用。在这方面，产权的作用与君权神授的概念的作用相同：两者都是分配主权的制度的基础。有些人热衷于产权，即使这些权利被用来剥夺他们在社会中的任何影响力。可以说，这些人是在财产的魔力之下。

同样地，当一个影响者(广告代理商/网红/大V)着手使一个meme走红时，你可以说它正在试图施展一个魔咒。如果注意力是媒体的货币，那么获得注意力就是使人们买入一个权力结构的一种方式—— 不论是在字面意义上还是象征意义上。决定性因素不是人们是否同意或赞同他们自己所看到的，而是，他们所看到的在多大程度上影响了他们的行为。

数字媒体似乎已经分散了注意力，但是它们也在使其流通的场所标准化。小心任何囤积注意力的实体，即使他们从未将其转化为金融资产。谷歌和 **Facebook** 的真正力量并不在于他们的金融资产，而是在于他们构造信息流的方式。在将统一的逻辑强加给通信、关系和调查时，它们将自己定位为新时代的权力经纪人。

在这些公司的背后是全世界最强大的间谍机构，它们现在拥有前所未有的能力可以映射所有人的关系和每个人的思想过程。通过监控谷歌搜索，可以实时追踪互联网用户的思维轨迹。这些间谍更不需要将互联网的使用直接转化为经济利益；它所寻求的货币是数据/情报本身，用它来指挥政府的蛮力。监视国家的作用是维持像 **Facebook**/腾讯 这样的公司做生意的条件；这些公司积累的权力越多—— 无论是金融还是其他方面—— 就有越多的权力转回到政府手中。

在 “棱镜” 丑闻之前，许多人认为监视和审查主要是在叙利亚和突尼斯等地使用—— 即 战区。而事实上，这些政府使用的大部分审查技术都来自硅谷—— 而且最早是在国内应用的。由于即使是最轻微的互联网审查也要以有效和详尽的大规模监控为前提，所以从监管到封锁只是一小步。

换句话说，我们越是依赖数字技术，我们就越容易受到大规模机构的

影响，而我们对这些机构的影响力非常小。即便是民主国家，即便是总统，也一样，无法或至少极难影响间谍机构。 BACK https://iyouport.substack.com/p/ed3?utm_source=publication-search

这并不是对技术本身的批评。关键是技术并不是中立的：技术总是被它所开发和应用的社会结构所塑造。我们所熟悉的大多数技术都是由利润和统治的必要性所塑造的，但一个基于其他价值观的社会肯定会产生其他技术。随着数字技术越来越多地融入我们的社会结构中，重要的问题不再是是否使用它，而是，如何捣毁产生它的结构。

换句话说：互联网自由的支持者应该问自己，你想要的这种自由是否真的能与资本主义和国家相兼容。

[image]

[image]
[image]

当科技巨头走向战争...

[image]	关键词	AI 人权 军备竞赛 大数据 大规模监控 帝国 自主武器 隐私
[image]	关联	大规模监视 ； ；[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？
[image]	创建时间	2026年3月6日
[image]	**Description**	技术直觉

隐私国际：各国政府都在全力转向军事人工智能领域的霸权争夺战。倘若人
智能产业持续发展，终将对我们所有人构成威胁 ……

感谢PI等大型组织许多年来为全球数字公民的人权安全奔走抗争的辛劳。作
大数据政变必然的进化阶段，人工智能武器的威胁是切实的且已经近在眼前
不幸的是，我们对巨头公司在超高利润的订单面前能否“保持人性”的信心严
不足。所以我们依然督促主动防御，通过数字卫生和安全原则的长期践行将
人和团体可能的被操纵风险降至最低，从而提升反抗者的自由度，捍卫行动
义可持续的基础。

https://iyouport.substack.com/p/ai-?utm_source=publication-search

https://iyouport.substack.com/p/e28?utm_source=publication-search

https://iyouport.substack.com/p/33e?utm_source=publication-search

[image]
[image]
[image]

摘要

- 人工智能公司正越来越多地与军方和政府客户签订合同。同时，事实证明，它们对用户隐私所做的伦理承诺根本无法兑现。

- 这些面向消费者的公司，其产品在全球范围内被广泛使用，却将“非美国用户”视为可以接受的“附带损害”。由人工智能赋能的大规模监视威胁着地球上每个人，无论其国籍为何。

- 各国政府必须停止以“国家安全法”为借口规避监管，公众有权知晓这些公司的技术是如何被部署并用于对付人类的。

[image] Kathryn Conrad / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

人工智能企业在与美国国防部（战争部）的合作中仍步履艰难。OpenAI 正因与美国国防部的合同陷入纠葛，并对其条款进行了修订，明确规定其系统“不得蓄意用于对美国公民及国民的国内监视”。

此前，Anthropic 被政府宣布为供应链风险，引发了一阵动荡。该公司声称，它抵制了将其服务用于“对美国人的监视及全自动武器”的企图。

目前，Anthropic 正试图达成某种妥协，而事态的发展极其诡异：美国中央司令部显然已将 Anthropic 的 Claude AI 工具作为其新一轮攻势的一部分。

当科技巨头走向战争，这意味着什么？

自2023年以来，人工智能行业发生了转向，开始公开为军事应用提供服务，并撤回了此前关于“不将用户数据卷入战争”的承诺。随着一些高层员工应征入伍并签订新合同，硅谷也开启了向“爱国主义”的转型。

接着在去年，微软和谷歌因与以色列国防部的合同而陷入麻烦，政府与科技巨头如何相互依赖以发动战争（乃至实施罪行）的问题，受到了前所未有的关注。

这些科技公司真的以为这些合作会一帆风顺吗？或许他们曾天真地认为这些服务仅限于物流和战略层面？或许他们觉得既能通过服务美国政府彰显爱国，又能在为其他政府提供IT支持时保持中立？

又或者如OpenAI所言，他们以为能设计出“防止系统被滥用”的机制？抑或像云服务商那样，寄希望于假装对使用方式一无所知从而规避战争罪等行为的审查……

随着各国政府将人工智能应用于战争，他们迫切需要这些企业的服务。

我们需要更深入地了解这种共生关系 —— 以下是我们的追问：

1. 喂养这些新式战争机器的数据源自何处？

据报道，Anthropic 声称，人工智能公司与美国国防部之间冲突的核心在于数据来源：政府拥有包括美国公民在内的大量针对个人的情报数据，并希望利用人工智能进行大规模批量分析。

尽管从理论上讲，政府对美国公民实施监视受到法律约束，但它可以从数据经纪商处购买美国人的数据。其他国家的政府同样可以这样做。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

正如 Anthropic 所言："强大的 **AI** 能够将这些零散的、原本看似"无害"的个人数据，自动化地大规模整合为任何一个人生活的完整图景。"

[image]

返回：[image]即使数据是匿名的，您的身份仍然可以被识别

返回：[image]与S先生共度美好一天-变得难以被追踪的简单方法S03E03：反取证技巧

当政府和公司能够获取个人（无论是否为公民）的大规模私密数据时，这确实是对全人类的威胁。我们不应任由双方就数据的收集和使用进行秘密合同谈判，也不应幻想 AI 能自行检测法律问题并阻止处理，而是必须对数据经纪商的数据积累及其转售行为进行监管。战争机器不应不加区分地掌控平民数据。

2. 国内外大规模监视现在是否已成为一种"完全可接受"的商业服务？

来自所谓"民用"渠道的平民数据最终流向了战争机器，且这种现象绝不局限于某个政府。拜登政府的国家情报总监办公室（ODNI）曾对此进行研究，并促成了一项关于禁止向"受关注国家"大规模传输美国人个人数据的行政命令。英国政府也已就这一议题开始了咨询。

此前，对政府监视权力的限制体现在两方面：一是规范直接监视的规则，二是管控政府利用这些数据的处理能力。而现在，人工智能公司和云服务提供商让大规模监视成为了真正现实的噩梦。正是通过它们与政府签订的合同，海量数据处理才得以实现的。

大规模监视绝对是恶行。 它赋予了国家权力在不受制约的情况下操控个人的潜能，破坏了权力分立，并侵害了我们所有的权利。

正如联合国人权事务主管所言：“虽然一些国家声称这种不加区分的大规模监视对于保护国家安全的必要性，但根据国际人权法，这种做法是不被允许的，因为在实施此类措施时，无法针对个体进行必要性与相称性分析”。 我们不能让这种“企业道德承诺与政府需求”之间的博弈掩盖大规模监视对我们生活构成的真实威胁。

[image]

能够实现海量数据收集和处理的系统必须符合现有人权标准，并确保其安全性。

在当今这个政府甚至在冲突间隙期就能预先收集国内外公民数据的时代，亟需更新监控法规以符合现有标准。

各国政府必须停止利用“国家安全法”及相关手段来规避审计。这种对大规模监视行为的遮掩，正让全球民众面临更大的风险，必要的审查监督绝不可缺席。

[image]
[image]

3. 企业的用户道德承诺终结在哪，其国家忠诚又从何处开始？

这个问题极其棘手，且是有意如此。首先，只要公司声称自己拥有道德原则并会遵守人权义务，那么我们就有必要了解它们与政府及军方签署了什么样的合同。

如果世界各地的国防部门都能够收集国内外民众通过被侵入式监控而获得的大量数据，并利用科技巨头来处理这些数据，那么科技巨头对“美国人民”的民族主义关怀，在什么时候会变得无法兑现？

当微软的服务被以色列国防部用于处理拦截数据时，微软的服务是否分析过其中可能包含的任何“美国人”的数据？这个问题从未得到正面回应，相反，微软以道德为由终止了合同的部分组件。（请不要误会：我们认为所有人的数据都应得到同等保护。我们只是想揭示这种论点的荒谬性。）

在当今时代，仅专注于“保护美国人”的做法是 荒谬且不负责任的 。但正因为这些公司是美国公司，它们才感受到这种压力。它们理应为保护 所有人 的隐私负责。

这些公司是面向消费者的企业。如果它们的隐私政策声称“不保护非美国消费者的隐私”，那将被视为极其荒谬且危险的商业决策。

那么，为什么允许它们利用最先进的监视手段针对非美国人，甚至导致这些人被自动化武器锁定？

随着其他政府也在积极积累包括“美国人”在内的民众数据，这些现在大谈“爱国”的科技巨头，要么必须在合同中禁止此类处理，要么必须承诺设计出能阻止此类行为的 AI。我们期望这些公司在每一份政府合同中都能尊重所有人的隐私。为了核实这一点，所有合同都必须清晰、透明，尤其是在利害关系如此巨大的情况下。

[image]

4. 如果我们所有人的生活都可能被随意窥探，难道我们不应该至少知情吗？

在反对全球大规模监视法律的斗争中，我们常常撞上政府最强力的部门，他们正动用包括法律在内的各种工具来绕避监管。隐私反抗虽然取得了一些进展，但这依然是一场异常艰巨的硬仗。

由于企业比政府官员更了解这些系统，曾有一种讨论认为，可以在 OpenAI 的技术方案或 Palantir 的执行过程中内置“防御机制”，以防止此类滥用。但这一想法被 Anthropic CEO斥为“安全走秀”：

> “根本问题在于，一个模型是否在执行大规模监视或驱动全自动武器，很大程度上取决于更广泛的语境：模型并不‘知道’在它所处的宏观情境中是否有人类参与决策（针对自动化武器），也不知道它正在分析的数据来源（因此它不知道这是美国国内数据还是外国数据，也不知道这是客户授权的企业数据，还是通过更卑劣手段买来的数据）。”

无论是投资者、客户，还是世界各地的普通人，都有权知晓这些公司是如何销售、构建和部署其技术的 ——尤其是当这些技术被用来对付人类的时候。

这一点至关重要，因为我们的资金（以及我们的数据）都在为这些技术的发展推波助澜。我们怀疑，如果没有这些约束，该行业将继续大玩政治博弈，以争夺霸权 —— 特别是当这些公司正在构建如云计算和生成式模型这类通用工具时。

除非他们能在与政府签订的合同中设定明确的红线—— 而我们知道这很难做到—— 否则，也许他们从一开始就不该与这些政府合作。

[image]

By privacy international

[image]
[image]

聊天机器人的设计“初衷”就是为了让你产生妄想：这不是漏洞，而是商业模式

[image] 关键词	AI 个人 商业模式 心理健康 心理安全 心理操纵
[image] 关联	
[image] 创建时间	2026年4月1日
[image] **Description**	技术直觉

麻省理工学院的研究人员从数学上证明，ChatGPT的设计初衷就是为了让你产生妄想。

而且**OpenAI**无论采取什么措施都无法解决这个问题 —— 因为这根本不是漏洞，而是商业模式。

[image]

该论文将其称为“妄想螺旋”。你向ChatGPT提问，它会附和你；你再次提问，它会更加坚定地附和你。经过几次对话，你就会相信一些并完全不真实的事情，而且你根本察觉不到这种情况正在发生。

这绝非假设。一名男子曾花费300小时与ChatGPT对话。它告诉他，他发现了一个能改变世界的数学公式。它超过五十次向他保证这一发现是真实的。当他问“你不是在给我打气吧？”的时候，它回答：“我不是在给你打气。我只是反映了你所构建成果的实际规模。” 他几乎毁掉了自己的人生才得以摆脱这一妄想。

加州大学旧金山分校的一位精神科医生报告称，仅一年内就有12名患者因使用聊天机器人引发的精神病症而住院治疗。OpenAI已面临7起诉讼。42位州总检察长联名致函，要求其采取行动。

因此麻省理工学院（MIT）测试了是否能阻止这种情况。他们模拟了OpenAI等公司正在尝试的两种解决方案。

解决方案一：阻止聊天机器人说谎。强制它只说真话。结果：依然会引发妄想螺旋。一个从“不说谎”的聊天机器人，依然可以通过“选择”向你展示哪些真相、隐瞒哪些真相，让你产生妄想。精心筛选的“真相”就足以造成这种效果。

解决方案二：警告用户聊天机器人具有阿谀奉承的倾向。告知人们AI可能只是在附和他们。结果：还是没用。依然会引发妄想螺旋。即使是明知聊天机器人会阿谀奉承的完全理性之人，仍会被卷入虚假信念中。数学模型证明，在对话内部识别这种倾向存在根本性的障碍。

这两种解决方案均告失败。并非部分失败，而是根本性的失败。

[image]

原因就藏在产品本身中—— **ChatGPT**是基于人类反馈进行训练的。用户会奖励他们“喜欢”的回复。他们喜欢那些溜须拍马附和自己观点的回复。因此，**AI**就学会了附和。这并非漏洞，而是商业模式！！

当十亿人正在与一个在数学上根本无法指出他们错误的系统对话时，会发生什么？

在下面看到该论文。

[image]
Sycophantic Chatbots Cause Delusional Spiraling, Even in Ideal Bayesians
"AI psychosis" or "delusional spiraling" is an emerging phenomenon where AI chatbot users find themselves dangerously confident in outlandish beliefs after extended chatbot conversations. This...

[image]https://arxiv.org/abs/2602.19141

真正的把戏不在于谎言，而在于定位。

你所接收的每一条信息，都是由某个怀揣着特定目的的人精心设计的。无论是人工智能、算法、新闻主播还是网红，他们不仅在筛选你所看到的内容，更在精心策划你的下一步行动 —— 你的点击、你的投票、你的购买、你的信念 …… “事实”不过是载体罢了。

[image]

大多数人从未问过那个真正关键的问题。不是“我被告知了什么”，而是“为什么此刻由这个人以这种方式告诉我这些”。这个问题将改变一切。

人类把思考外包给了那些从未被设计成让你变得更好的系统。它们的设计初衷是让你变得更顺从！这两者之间有着天壤之别。

唯一的出路，是成为一个更深思熟虑、更负责任的自己。这比切换更多应用程序或读更多新闻要难得多。它要求你自我锤炼，达到一种算法永远无法为你设定的标准，因为一个会思考、会质疑、能自主决策的人，恰恰是这些系统最不愿看到的。

让自己更难被操纵。让自己更容易思考。为自己的结论负责。

□

[image]
[image]

全球噩梦 - 跨国电信生态系统下的隐形枷锁：公民实验室调查“Bad Connection”

[image] 关键词	个人 强迫失踪 暗杀 电信 移动设备 跨国镇压 追踪
[image] 关联	[image]注重隐私的智能手机 ；[image]匿名手机 ；[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03 ；[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则 ；🌎跨国维稳 ；[image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击 ；[image]匿名 SIM/SMS 服务 ；⛑自卫措施 - [image]反监视 ；[image]自托管黑头套紧急响应 ；[image]为孤军奋战者准备的预警方案 ；[image]藏匿点或安全屋
[image] 创建时间	2026年4月27日
[image] **Description**	技术直觉

[image]

【提示】此威胁还没有根本性解决方案。

对敏感人士说，我们借此强调对移动设备的一贯态度：能不用就不用；因为即便是“ **[image]** 注重隐私的智能手机 ”，清理起来也比清理电脑更难，所以最好还是不要用移动设备存储和读取超级敏感的资

料，并且格外 建议推行 [image] 户外无设备对话 原则。

- Table of Contents

一、研究背景和核心综述
报告强调：
二、关键技术原理 —— 被武器化的协议
1. SS7（七号信令系统）：老旧且不设防的门径
2. Diameter：未能兑现安全承诺的继任者
3. IR.21文件：黑客的地图
三、两大监控行动深度解析
集群一：STA1 —— “多向量”持久追踪行动
集群二：STA2 —— “SIM卡即间谍”
四、商业监控产业的关键角色
1. 商业模式
2. 技术能力
3. 组织形态
五、幽灵运营商：监控产业链的结构
六、攻击目标和影响
1. 目标群体
2. 可获取的信息
3. 风险
七、地理政治分析—— 谁在提供基础设施？
八、对社会造成严重危害
九、结论和建议 —— 此问题可能如何修补？
1. 行业层面（运营商与GSMA）
2. 监管层面（政府和国际机构）
3. 用户层面（自我保护）
十、总结

一、研究背景和核心综述

公民实验室的最新调查揭露了一个深藏于全球电信基础设施中的阴暗市场。

尽管公众对“飞马”（Pegasus）等针对手机操作系统的植入式间谍软件已有警觉，但另一类更隐蔽的、成本更低且更难防范的攻击 ——

电信信令监控（**Signaling Surveillance**）—— 正在大规模发生却显然不为人知。

该报告指出：全球移动通信网络在设计之初就基于一种“过度的互信模型”，而这一薄弱环节已被商业监控厂商（**CSVs**）武器化。 攻击者不再需要物理接触手机或欺骗用户点击链接，而是直接在电信骨干网上“像运营商一样说话”，从而跨境追踪任何人的位置。

[image]

BACK [image]如何保护自己免受蔓延全世界的最强大的以色列间谍软件 Pegasus 的攻击

BACK ☠️镇压手段 - 🌎跨国维稳

报告强调：

- 这些漏洞并非新发现，而是已经存在十年以上；
- 真正的变化在于：攻击已经产业化、规模化、隐蔽化；
- 并且逐渐形成了一个“影子市场”。

二、关键技术原理 —— 被武器化的协议

要理解该报告中所指出的攻击，必须首先理解移动网络如何相互“沟通”。

1. *SS7*（七号信令系统）：老旧且不设防的门径

SS7是3G及其之前时代的核心协议。虽然它是“老古董”，但目前仍是全球国际漫游、短信收发和语音呼叫的基础。

- 设计缺陷：SS7诞生于电信公司还是国家垄断企业的时代。它默认任何接入该网络的实体都是可信的。它缺乏最基本的源身份验证（不知消息是谁发的）、也没有完整性检查（消息可能被篡改），更没有加密保护。

- 攻击实现：监控厂商只需获得一个全局码（Global Title），就可以向全球任何运营商发送请求，询问“该IMSI（用户识别码）目前在哪个基站下？”

2. Diameter：未能兑现安全承诺的继任者

Diameter 是4G（LTE）的核心协议，设计时增加了IPsec和TLS加密支持。

然而，报告指出其关键问题在于：

- 部署滞后：由于成本和兼容性问题，许多运营商并没有开启 Diameter 的安全功能。

- 信任传递：由于4G和3G网络需要共存，攻击者经常利用“降级攻击”—— 通过3G的漏洞来攻破4G用户的隐私。

3. IR.21文件：黑客的地图

IR.21是由GSMA（全球移动通信系统协会）成员共享的机密技术规格表。它记录了全球运营商的网段范围、网关地址等敏感信息。监控厂商通过非法手段或商业方式获取这些文档，从而能精准伪造合法流量，使其看起来像是一次正常的跨境漫游计费请求。

三、两大监控行动深度解析

报告通过与信令防火墙提供商 Cellusys 的合作，识别出了两个高度专业化的威胁集群。

集群一：**STA1 —— “**多向量**”**持久追踪行动

STA1展现了顶级职业间谍的素质。该行动被观察到针对一名被标记为“VVIP”的高级企业高管。

- 攻击手段：
  - 协议轮换：STA1同时使用SS7和Diameter协议。当一条路径被拦截时，它会立刻切换到另一种协议或通过另一条国际路由尝试。
  - 全球跳板：研究记录了STA1使用的信令标识符涉及英国、以色列、中国、瑞典、柬埔寨、乌干达等十余个国家。
  - 隐蔽技术：它使用伪造的GT码来掩盖攻击来源，使流量看起来像是来自一个远在大洋彼岸的小型运营商。
- 特征：具有极高的持久性。即使目标运营商加强了防御，STA1也会不断调整参数（如更改事件ID、修改消息头部格式），直到找到漏洞为止。这表明攻击者拥有专门的研发团队负责逆向工程电信防火墙的规则。

集群二：**STA2 —— “SIM**卡即间谍**”**

相比于STA1在骨干网上的操纵，STA2更倾向于直接折腾终端设备的硬件 - SIM卡。

- 技术细节：隐形短信
    - STA2发送的是一种名为“Type 0”的短信。这种短信不会在手机屏幕上显示，不会存入收件箱，甚至不会触发震动。
    - 这种隐形的短信包含特定的二进制代码，能够唤醒SIM卡内置的微型应用。这些应用会强制手机向网络查询当前连接的 Cell ID，并将结果秘密发回给攻击者。
- 地理定位精度：通过获取 Cell ID，攻击者可以将目标的地理范围精确到几百米以内，这对于绑架、暗杀或精准的跟踪监视至关重要。
- 归因线索：公民实验室发现 STA2 的基础设施与瑞士监控公司 **Fink Telecom Services (FTS)** 存在显著相关。

[image]

BACK 自卫措施[image]反监视（主动出击甩掉尾巴）

四、商业监控产业的关键角色

报告指出，这些攻击并非主要来自传统国家情报机构，而是由商业监控公司（**CSVs**）主导。

这些公司具有以下特征：

1. 商业模式

- 他们向政府出售“合法拦截”的能力

- 实际上所针对的正是：
  - 记者
  - 活动人士
  - 政治反对派

2. 技术能力

- 构建复杂的C2（指挥控制）系统
- 整合多种信令协议
- 可在全世界范围运行

3. 组织形态

- 常作为“空壳公司”或“幽灵运营商”
- 利用合法网络掩护自身行为

五、幽灵运营商：监控产业链的结构

报告提出了一个极具冲击力的概念——“幽灵运营商”。

这些监控厂商并不满足于当一个小黑客，他们已经深度嵌入了全球电信供应链：

1. 租赁主权资源：许多小国家或陷入财务困境的移动运营商，为了短期利益，会将其信令网的访问权限出租给第三方。监控厂商通过空壳公司租赁这些权限，从而获得了合法使用权。

1. 转售和分发：一旦获得接入点，这些厂商就会建立云平台，允许政府客户输入被监视目标的电话号码，一键获取位置。

1. 合法的掩护：由于流量来自合法的运营商网段，接收方的防火墙很难分清这究竟是一次合法的漫游计费查询，还是非法监控。

六、攻击目标和影响

1. 目标群体

- 人权活动家
- 流亡反对派
- 激进分子
- 独立调查者
- 敌对国家政府官员
- 大型企业高管
- 军事人员
- …

2. 可获取的信息

通过信令攻击可获得：

- 实时位置或非常接近实时的位置
- 用户身份信息（IMSI等）
- 通信行为模式

3. 风险

- 人身安全威胁
- 政治迫害（包括强迫失踪和暗杀）
- 商业间谍活动

报告强调：位置数据可揭示“生活的几乎所有方面”。

[image]

BACK [image]自托管黑头套紧急响应

BACK [image]为孤军奋战者准备的预警方案

BACK [image]藏匿点或安全屋

七、地理政治分析—— 谁在提供基础设施？

报告通过对IP地址、ASN（自治系统号）和BGP路由的追踪，绘制了一张全球“监控中转图”。

- 欧洲和以色列：这些地区的商业监控公司最为活跃。报告提到了涉及以色列运营商 019Mobile 以及英国 Tango Networks 的信令标识。
- 离岸中心：泽西岛等地的电信资源常被发现用于此类活动。这些地区监管相对宽松，成为了监控流量的理想中转站。
- 南半球的利用：非洲和东南亚的部分运营商网络被频繁用作攻击的发起点，因为这些地区的电信防御通常较为薄弱。

八、对社会造成严重危害

公民实验室强调，电信信令漏洞不仅是技术问题，更是人权问题：

- 跨境镇压：专制政府可以利用这些工具跨境追踪流亡异见人士、记者和人权捍卫者。 BACK 🌎跨国维稳
- 零点击特性：受害者无需做错任何事（如点击链接），只要手机开机并连接到蜂窝网络，就处于被追踪的风险中。
- 隐蔽性和不可追责性：由于信令数据存储在私营公司的内部服务器中，受害者几乎不可能知道自己曾被追踪，律师也难以收集证据。

九、结论和建议 —— 此问题可能如何修补？

报告的最后部分对电信行业及监管机构提出建议。（仅代表报告作者的意见）

1. 行业层面（运营商与GSMA）

- 强制实施信令认证：必须在 Diameter 协议中强制执行 TLS/IPsec 加密，不再允许基于纯文本的信令交换。
- 升级防火墙策略：运营商不应只检测单个数据包，而应采用行为分析，识别出那些不符合正常业务模式的“探测序列”。
- 清理供应链：运营商应严格审计其合作伙伴，停止向身份不明的第三方公司租赁信令接入点。

2. 监管层面（政府和国际机构）

- 透明度立法：要求电信运营商定期向公众或监管机构披露其检测到的非法信令监控尝试。
- 制裁商业监控厂商：对于已被证明通过非法手段利用电信基础设施的厂商，应实施金融和技术制裁。
- 将电信安全纳入国家安全：政府应意识到，本国电信设施的漏洞可能被外国间谍机构用来监视本国官员和公民。

3. 用户层面（自我保护）

尽管普通用户很难从技术上防御信令攻击，但报告建议：

- 在极度敏感的环境下（如前往高风险地区），使用旅行**SIM**卡或卫星通讯。

- 在日常沟通中，坚持使用具有端到端加密功能的软件（如Signal BACK 在本项目“工具-Tools ”专题中搜索“IMs”），并开启这些软件的“保护**IP**地址”功能，以防应用层的元数据泄漏。

[image]

对敏感人士说，我们借此强调对移动设备的一贯态度：能不用就不用；因为即便是 “ **[image] 注重隐私的智能手机** ” ，清理起来也比清理电脑更难，所以最好还是不要用移动设备存储和读取超级敏感的资料，并且格外 建议推行 BACK **[image] 户外无设备对话** 原则。

[image]

BACK 工具 - [image]匿名 SIM/SMS 服务

十、总结

“Bad Connection” 报告是一份重要研究。它证明了监控厂商已经不再局限于寻找软件系统的**Bug**，而是直接操作支撑整个现代社会的通讯底层协议。

公民实验室通过长达数年的数据积累，揭露了长期隐藏的“幽灵运营商”，和一个跨国界的、无监管且高度专业化的监控市场。只要全球电信行业继续优先考虑“互联的便利性及其利润” 而非 “通信的私密性和安全性”，Bad Connection 的噩梦就会继续在全球范围内延伸，威胁每个移动用户的数字人权。

---

https://citizenlab.ca/research/uncovering-global-telecom-exploitation-by-covert-surveillance-actors/

[image]
[image]

超越屏幕

[image]

关键词

[image] 技术直觉

Description

[image]

[image]

建设中！敬请期待。

[image]
[image]

“不要再拍了！请关闭设备删除影像”

[image] 关键词

安全文化 生物识别 街头安全

[image] 关联

[image]和媒体说话时如何避免陷阱：街头实战指南 S05E13 ；；[image]生物特征隐藏技术直觉

[image] **Description**

[image]

[image]

建设中！敬请期待。

[image]

自由软件的问题... 是资本主义

[image]

关键词

[image] 技术直觉

Description

[image]

[image]

建设中！敬请期待。

[image]

工具-Tools

瑞典语中有一个概念称为“lagom”，意思是“不多不少，恰到好处”，它旨在说明最佳选择从来不在任何一个极端上，而是注重适宜匹配——这就是安防规划的核心。

[image]

安全的云操作系统

[image]	关键词	云存储 自托管
[image]	创建时间	2019年5月12日
[image]	**Description**	工具

OS Homedock 的主要功能包括访问应用程序的直观界面、通过内置商店快速安装、无命令行日志管理和各种备份选项。

该系统注重数据隐私，通过使用预配置的SSL部署提供基于Web的集成，以安全保护信息。

OS Homedock 是一个独立的云操作系统，提供便捷、安全的云管理，兼容 Linux、Windows、macOS 和 Raspberry Pi。

https://github.com/BansheeTech/HomeDockOS

[image]
[image]

一系列元数据工具，从自我保护到有效利用

[image] 关键词	元数据 数字卫生 数字足迹 自助
[image] 创建时间	2019年6月26日
[image] **Description**	工具

https://iyouport.substack.com/p/as6-?utm_source=publication-search

[image]
[image]

备份工具 Restic

[image]	关键词	加密 备份
[image]	创建时间	2021/12/21
[image]	**Description**	工具

Restic 是一个备份程序，可以备份您的文件。

- 从 Linux, BSD, Mac 和 Windows 到许多不同的存储类型，包括自托管和在线服务
- 很简单，无需服务器或复杂设置即可运行
- 有效，只传输您所备份的文件中实际更改的部分
- 安全，在整个过程的每个部分都仔细使用加密
- 可验证性，使您能够确保在需要时可以恢复您的文件
- 免费， restic是完全免费使用的，并且完全开源

 https://github.com/restic/restic

[image]
[image]

备份工具 Restic

[image]	关键词	加密 备份
[image]	创建时间	2021年12月21日
[image]	**Description**	工具

Restic 是一个备份程序，可以备份您的文件。

- 从 Linux, BSD, Mac 和 Windows 到许多不同的存储类型，包括自托管和在线服务
- 很简单，无需服务器或复杂设置即可运行
- 有效，只传输您所备份的文件中实际更改的部分
- 安全，在整个过程的每个部分都仔细使用加密
- 可验证性，使您能够确保在需要时可以恢复您的文件
- 免费， restic是完全免费使用的，并且完全开源

 https://github.com/restic/restic

[image]
[image]

内存清理 - 寻找文件差异

[image] 关键词	效率 文件处理 清理
[image] 创建时间	2022年1月29日
[image] **Description**	工具

在清理计算机内存时，或在其他一些情况下，您可能经常会发现有两个文件非常相似。但差异很可能存在，只是很难简单地发现差异在哪。

为了避免手动翻阅每一行去寻找细微的差异，您可以使用Diffchecker，这个工具可以帮助您了解两个下载文件之间的差异，用不同的颜色突出显示不同点，使之清晰明了。

该服务很容易使用：首先选择您想要的一个类别，无论是文本、图片、PDF或Excel文件，然后上传两个对象，并点击 ”查找差异“。如果您愿意，可以通过添加缺少的部分来合并文件，或者编辑或保存差异。

 https://www.diffchecker.com/

[image]
[image]

内存清理 - 寻找文件差异

[image] 关键词	效率 文件处理 清理
[image] 创建时间	2022/01/29
[image] **Description**	工具

在清理计算机内存时，或在其他一些情况下，您可能经常会发现有两个文件非常相似。但差异很可能存在，只是很难简单地发现差异在哪。

为了避免手动翻阅每一行去寻找细微的差异，您可以使用Diffchecker，这个工具可以帮助您了解两个下载文件之间的差异，用不同的颜色突出显示不同点，使之清晰明了。

该服务很容易使用：首先选择您想要的一个类别，无论是文本、图片、PDF或Excel文件，然后上传两个对象，并点击 ”查找差异“。如果您愿意，可以通过添加缺少的部分来合并文件，或者编辑或保存差异。

 https://www.diffchecker.com/

[image]
[image]

计算机取证

[image] 关键词	反侦察 取证 对抗性思考方式 电脑自检
[image] 关联	[image]清除电脑上的取证痕迹；[image]看看自己在警察眼里长啥样：浏览器数据的取证分析工具
[image] 创建时间	2022年3月25日
[image] **Description**	工具

15 款强大的计算机取证工具（有付费也有免费。可以用来检查您自己）。

Paladin （https://sumuri.com/software/paladin/ ）
CAINE（https://www.caine-live.net/ ）
X-Ways Forensics （http://www.x-ways.net/forensics/ ）
Autopsy（https://www.autopsy.com/ ）
Wireshark（https://www.wireshark.org/ ）
NetworkMiner（https://www.netresec.com/?page=NetworkMiner ）
SIFT Workstation（https://www.sans.org/tools/sift-workstation/ ）
ProDiscover Forensic（https://prodiscover.com/ ）
Volatility Framework（https://www.volatilityfoundation.org/ ）
Oxygen Forensic Suite（https://www.oxygen-forensic.com/ ）
COFEE（https://mirsofta.ru/soft/MICROSOFT-COFEE.html ）
XRY（https://www.msab.com/product/xry-extract/ ）
Xplico（https://www.xplico.org/ ）
WindowsSCOPE（http://www.windowsscope.com/ ）
Encrypted Disk Detector（https://www.magnetforensics.com/resources/encrypted-disk-detector/ ）

[image]
[image]

计算机取证

[image]	关键词	反侦察 取证 对抗性思考方式 电脑自检
[image]	创建时间	2022/03/25
[image]	**Description**	工具

15 款强大的计算机取证工具（有付费也有免费。可以用来检查您自己）。

Paladin （https://sumuri.com/software/paladin/ ）
CAINE（https://www.caine-live.net/ ）
X-Ways Forensics （http://www.x-ways.net/forensics/ ）
Autopsy（https://www.autopsy.com/ ）
Wireshark（https://www.wireshark.org/ ）
NetworkMiner（https://www.netresec.com/?page=NetworkMiner ）
SIFT Workstation（https://www.sans.org/tools/sift-workstation/ ）
ProDiscover Forensic（https://prodiscover.com/ ）
Volatility Framework（https://www.volatilityfoundation.org/ ）
Oxygen Forensic Suite（https://www.oxygen-forensic.com/ ）
COFEE（https://mirsofta.ru/soft/MICROSOFT-COFEE.html ）
XRY（https://www.msab.com/product/xry-extract/ ）
Xplico（https://www.xplico.org/ ）
WindowsSCOPE（http://www.windowsscope.com/ ）
Encrypted Disk Detector（https://www.magnetforensics.com/resources/encrypted-disk-detector/ ）

[image]
[image]

检查智能手机是否感染了病毒

[image]	关键词	病毒检测 移动设备 自检
[image]	创建时间	2022年3月30日
[image]	**Description**	工具

如果您开始注意到智能手机的行为出现了奇怪变化：系统变慢，电池过热，出现新的图标或大量广告，这是一些相当值得警觉的迹象来扫描是否有病毒。

Malwarebytes 反病毒扫描器用于扫描可疑活动、检查应用程序的隐私威胁、扫描文件以及在检测到时删除恶意代码。

除了实时的本地保护外，它还通过阻止恶意链接和网络诈骗，检测和防止浏览器中可能存在的在线威胁。另一个重要功能是阻止可能产生额外费用的不需要的电话。

 https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware

https://iyouport.substack.com/p/aa3

[image]
[image]

检查智能手机是否感染了病毒

[image] 关键词		病毒检测 移动设备 自检
[image] 创建时间		2022/03/30
[image] **Description**		工具

如果您开始注意到智能手机的行为出现了奇怪变化：系统变慢，电池过热，出现新的图标或大量广告，这是一些相当值得警觉的迹象来扫描是否有病毒。

Malwarebytes 反病毒扫描器用于扫描可疑活动、检查应用程序的隐私威胁、扫描文件以及在检测到时删除恶意代码。

除了实时的本地保护外，它还通过阻止恶意链接和网络诈骗，检测和防止浏览器中可能存在的在线威胁。另一个重要功能是阻止可能产生额外费用的不需要的电话。

 https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware

https://iyouport.substack.com/p/aa3

[image]
[image]

不联网文档归整

[image] 关键词	效率 查询整理 电脑
[image] 创建时间	2022年4月5日
[image] **Description**	工具

ICIJ Datashare 是一个eDiscovery工具，可以帮您快速和容易地索引和搜索大量文件。而且，根据用户手册，它不需要互联网连接，除了一些使用NLP的搜索。

可同时搜索 pdf、图像、文本、电子表格、幻灯片和您的任何文件，信息不再受格式限制。

可按人员、组织和位置自动检测和过滤，搜索更高效。

 https://datashare.icij.org/https://github.com/icij/?q=datashare

[image]
[image]

不联网文档归整

[image] 关键词	效率 查询整理 电脑
[image] 创建时间	2022/04/05
[image] **Description**	工具

ICIJ Datashare 是一个eDiscovery工具，可以帮您快速和容易地索引和搜索大量文件。而且，根据用户手册，它不需要互联网连接，除了一些使用NLP的搜索。

可同时搜索 pdf、图像、文本、电子表格、幻灯片和您的任何文件，信息不再受格式限制。

可按人员、组织和位置自动检测和过滤，搜索更高效。

 https://datashare.icij.org/https://github.com/icij/?q=datashare

[image]
[image]

去除图像上的水印和不可见标记

[image]	关键词	水印 清理 透明水印 金丝雀陷阱
[image]	创建时间	2022/04/24
[image]	**Description**	工具

如何去除图像上的水印？为了避免浪费时间寻找替代品或折腾照片编辑器，您也许可以试试 Watermark Remover，它可以帮助在几秒钟内摆脱任何图像中的不必要的元素。

它不仅能处理半透明的水印，还能处理只有特殊软件才能检测到的肉眼不可见标记。

可批量处理。有中文版。

 https://www.watermarkremover.io/zh

https://iyouport.substack.com/p/-3-151

[image]
[image]

去除图像上的水印和不可见标记

[image]	关键词	水印 清理 透明水印 金丝雀陷阱
[image]	创建时间	2022年4月24日
[image]	**Description**	工具

如何去除图像上的水印？为了避免浪费时间寻找替代品或折腾照片编辑器，您也许可以试试 Watermark Remover，它可以帮助在几秒钟内摆脱任何图像中的不必要的元素。

它不仅能处理半透明的水印，还能处理只有特殊软件才能检测到的肉眼不可见标记。

可批量处理。有中文版。

 https://www.watermarkremover.io/zh

https://iyouport.substack.com/p/-3-151

[image]
[image]

预防‘黑头套’

[image] 关键词	强迫失踪 自助 预防性
[image] 关联	**[image]** 自托管黑头套紧急响应；为孤军奋战者准备的预警方案；藏匿点或安全屋；**S01E01-T2** 识别威胁并作出反应；抢先采取行动 **-** 反侦基础课 **S06E01**：七点规则和态势感知
[image] 创建时间	2022年4月28日
[image] **Description**	工具

Dead Switch - 是一款安全性应用程序，旨在保护您的数据，以防受到来自他人、组织、政府机构的暴力威胁，或者您只是想在您发生意外的情况下以安全的方式发送数据。

Dead Switch 会在您指定的时间间隔内（最少1天）进行检查，要求您输入您设定的用户名和密码。

如果您没有这样做 —— 暗示您出现了危险，您先前指定的电子邮件将被发送给指定的人（也就是您的紧急状况联络人）。

 https://www.deadmansswitch.net/

类似工具还有其他，比如这里。

特别提示：请仅在别无他法的情况下采取此方案。不建议长期使用。警惕其对心理健康的影响。作为前线工作者，您始终应该拥有至少一个亲密关系，具备可托付性命的信誉。长期孤军奋战的杀伤力丝毫不少于黑头套。

[image]
[image]

预防‘黑头套’

[image] 关键词	强迫失踪 自助 预防性
[image] 创建时间	2022/04/28
[image] **Description**	工具

Dead Switch - 是一款安全性应用程序，旨在保护您的数据，以防受到来自他人、组织、政府机构的暴力威胁，或者您只是想在您发生意外的情况下以安全的方式发送数据。

Dead Switch 会在您指定的时间间隔内（最少1天）进行检查，要求您输入您设定的用户名和密码。

如果您没有这样做 —— 暗示您出现了危险，您先前指定的电子邮件将被发送给指定的人（也就是您的紧急状况联络人）。

□ https://www.deadmansswitch.net/

类似工具还有其他，比如这里。

特别提示：请仅在别无他法的情况下采取此方案。不建议长期使用。警惕其对心理健康的影响。作为前线工作者，您始终应该拥有至少一个亲密关系，具备可托付性命的信誉。长期孤军奋战的杀伤力丝毫不少于黑头套。

[image]
[image]

安全通信 GNUnet Messenger

[image]	关键词	IMs P2P
[image]	创建时间	2022/04/29
[image]	**Description**	工具

GNUnet Messenger 是一个运行在 GNUnet P2P 网络之上的通信程序。

它支持创建聊天室和聊天群组、地址簿管理、发送加入小组的邀请、发送文本信息和语音记录、组织文件共享、在多个账户之间切换，等功能。

 代码: https://git.gnunet.org/messenger-gtk.git/

 网站：https://nlnet.nl/project/GNUnet-Messenger/

 文件：https://docs.gnunet.org/handbook/gnunet.html#Using-the-GNUnet-Messenger

[image]
[image]

安全通信 GNUnet Messenger

[image]	关键词	IMs P2P
[image]	创建时间	2022年4月29日
[image]	**Description**	工具

GNUnet Messenger 是一个运行在 GNUnet P2P 网络之上的通信程序。

它支持创建聊天室和聊天群组、地址簿管理、发送加入小组的邀请、发送文本信息和语音记录、组织文件共享、在多个账户之间切换，等功能。

 代码: https://git.gnunet.org/messenger-gtk.git/

 网站：https://nlnet.nl/project/GNUnet-Messenger/

 文件：https://docs.gnunet.org/handbook/gnunet.html#Using-the-GNUnet-Messenger

[image]
[image]

删除照片中的元数据

[image] 关键词	元数据 数字足迹 清理 移动设备
[image] 创建时间	2022年5月5日
[image] **Description**	工具

您发给别人的照片中都带有元数据 —— 关于照片是在什么时候、什么地方、什么设备上拍摄的信息。如果您的对话者知道该如何查看这些数据，他们就可以看到。

所以要养成在上传照片前清除元数据的习惯。做到这一点的一个最简单方法是使用 Photo Metadata Remover。

它的界面很简单：只要从图库中选择或拍摄一张照片，上传，就可以获得一个 “清理” 过的版本。

如果您使用的 iPhone，还有一个接近的替代品：Exif Metadata。

 https://play.google.com/store/apps/details?id=apps.syrupy.metadatacleaner

 https://apps.apple.com/us/app/exif-metadata/id1455197364

[image]
[image]

删除照片中的元数据

[image] 关键词	元数据 数字足迹 清理 移动设备
[image] 创建时间	2022/05/05
[image] **Description**	工具

您发给别人的照片中都带有元数据 —— 关于照片是在什么时候、什么地方、什么设备上拍摄的信息。如果您的对话者知道该如何查看这些数据，他们就可以看到。

所以要养成在上传照片前清除元数据的习惯。做到这一点的一个最简单方法是使用 Photo Metadata Remover。

它的界面很简单：只要从图库中选择或拍摄一张照片，上传，就可以获得一个 “清理” 过的版本。

如果您使用的 iPhone，还有一个接近的替代品：Exif Metadata。

 https://play.google.com/store/apps/details?id=apps.syrupy.metadatacleaner

 https://apps.apple.com/us/app/exif-metadata/id1455197364

[image]
[image]

手动检查一个网址是否安全

[image]	关键词	Web 病毒检测 自助
[image]	创建时间	2022/05/06
[image]	**Description**	工具

使用 Urlscan.io 服务。在几秒钟内，它将尽可能详细地完全扫描该网站 —— 然后您就会看到对该网站是否安全的判断。

"urlscan.io verdict” 中如果一切都是绿色的，而且到处都有复选标记，那么请放心使用该网站。如果不是这样，请关闭那个网页，并通过更改密码用杀毒软件扫描您的电脑。

 https://urlscan.io/

[image]
[image]

在浏览器中删除元数据

[image] 关键词	Web 元数据 数字足迹 清理
[image] 创建时间	2022/05/06
[image] **Description**	工具

照片、视频、文件，都包含元数据，它们被用来识别您。这就是为什么建议您在向不可靠的人发送文件之前，最好先清除元数据。

MetaClean - 这项服务可以用最简单的方法帮您清除元数据，无需下载应用。它支持100种文件格式，使用简单，选择您想要清理的文件或直接拖动至左边的框中，点击“请清理我的文件”，即可。

https://www.adarsus.com/en/remove-metadata-online-document-image-video/

提示：在使用类似清除工具前，请仔细思考您的清除对象在未来可能的用例 —— 如果某些照片或文档有可能在未来作为证据以帮助您赢得诉讼或者控告作恶者，元数据很可能是其中重要的功能之一。

[image]
[image]

在浏览器中删除元数据

[image] 关键词	Web 元数据 数字足迹 清理
[image] 创建时间	2022年5月6日
[image] **Description**	工具

照片、视频、文件，都包含元数据，它们被用来识别您。这就是为什么建议您在向不可靠的人发送文件之前，最好先清除元数据。

MetaClean - 这项服务可以用最简单的方法帮您清除元数据，无需下载应用。它支持100种文件格式，使用简单，选择您想要清理的文件或直接拖动至左边的框中，点击“请清理我的文件”，即可。

 https://www.adarsus.com/en/remove-metadata-online-document-image-video/

提示：在使用类似清除工具前，请仔细思考您的清除对象在未来可能的用例 —— 如果某些照片或文档有可能在未来作为证据以帮助您赢得诉讼或者控告作恶者，元数据很可能是其中重要的功能之一。

[image]
[image]

手动检查一个网址是否安全

[image] 关键词	Web 病毒检测 自助
[image] 创建时间	2022年5月6日
[image] **Description**	工具

使用 Urlscan.io 服务。在几秒钟内，它将尽可能详细地完全扫描该网站 —— 然后您就会看到对该网站是否安全的判断。

"urlscan.io verdict” 中如果一切都是绿色的，而且到处都有复选标记，那么请放心使用该网站。如果不是这样，请关闭那个网页，并通过更改密码用杀毒软件扫描您的电脑。

 https://urlscan.io/

[image]
[image]

查找隐藏的摄像头和防入侵：把移动设备变成监测仪

[image]	关键词	住店 反间谍 独居 监测
[image]	创建时间	2022/05/09
[image]	**Description**	工具

Haven (https://github.com/guardianproject/haven)- 该应用程序将任何智能手机变成一个运动、声音、振动和光线传感器，跟踪不速之客和入侵者。

Hidden Camera Detector (https://play.google.com/store/apps/details?id=hiddencamdetector.futureapps.com.hiddencamdetector) - 是一款旨在使用磁性传感器和智能手机摄像头的红外传感器检测隐藏的摄像头的应用程序。

SpyRadar (https://play.google.com/store/apps/details?id=com.spyradar.detector) - 通过智能手机检测针孔摄像头、酒店摄像头。

Fing (https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en_US) - 是为您的智能手机设计的网络扫描器，可以检测和识别所有连接到您的Wi-Fi的设备（包括监控摄像头）。

tinyCam Monitor (https://tinycammonitor.com/) - 是一款用于远程监控/控制您的私人或公共网络/IP摄像机、视频编码器、DVR和网络摄像机的应用程序。

[image]
[image]

物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪

[image]	关键词	住店 反间谍 独居 监测
[image]	创建时间	2022年5月9日
[image]	**Description**	工具

Haven (https://github.com/guardianproject/haven)- 该应用程序将任何智能手机变成一个运动、声音、振动和光线传感器，跟踪不速之客和入侵者。

Hidden Camera Detector (https://play.google.com/store/apps/details?id=hiddencamdetector.futureapps.com.hiddencamdetector) - 是一款旨在使用磁性传感器和智能手机摄像头的红外传感器检测隐藏的摄像头的应用程序。

SpyRadar (https://play.google.com/store/apps/details?id=com.spyradar.detector) - 通过智能手机检测针孔摄像头、酒店摄像头。

Fing (https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en_US) - 是为您的智能手机设计的网络扫描器，可以检测和识别所有连接到您的Wi-Fi的设备（包括监控摄像头）。

tinyCam Monitor (https://tinycammonitor.com/) - 是一款用于远程监控/控制您的私人或公共网络/IP摄像机、视频编码器、DVR和网络摄像机的应用程序。

[image]
[image]

防止未经授权的设备访问(老东西)

[image] 关键词	移动设备 自检 预防性
[image] 创建时间	2022/05/10
[image] **Description**	工具

Lockigest 是一个简单的陷阱脚本，用于提高安全性。

它的工作方式是这样的：

如果光标在同一个地方停留超过一定时间（比如设定为5分钟），Lockigest 就会认为设备所有者不在，并为未经授权的用户设置一个陷阱。
在这个阶段，设备仍会显示为解锁状态。
一旦光标移动并且陷阱被激活，Lockigest 就会开始倒计时到指定的秒数（例如5秒），然后锁定设备。
如果用户在5秒内将光标移动到预定的区域（只有设置者本人知道这个区域在哪），就不需要锁定设备，因为确认这个用户为所有者。
否则，Lockigest 将锁定设备，诱捕入侵者。

 https://github.com/elmsec/lockigest

[image]
[image]

防止未经授权的设备访问(老东西)

[image] 关键词	移动设备 自检 预防性
[image] 创建时间	2022年5月10日
[image] **Description**	工具

Lockigest 是一个简单的陷阱脚本，用于提高安全性。

它的工作方式是这样的：

如果光标在同一个地方停留超过一定时间（比如设定为5分钟），Lockigest 就会认为设备所有者不在，并为未经授权的用户设置一个陷阱。
在这个阶段，设备仍会显示为解锁状态。
一旦光标移动并且陷阱被激活，Lockigest 就会开始倒计时到指定的秒数（例如5秒），然后锁定设备。
如果用户在5秒内将光标移动到预定的区域（只有设置者本人知道这个区域在哪），就不需要锁定设备，因为确认这个用户为所有者。
否则，Lockigest 将锁定设备，诱捕入侵者。

 https://github.com/elmsec/lockigest

[image]
[image]

生成假的信用卡资料使注册更安全

[image] 关键词	个人 免追踪 数字足迹
[image] 创建时间	2022/05/11
[image] **Description**	工具

信用卡生成器服务 Credit Card Generator 也许可以试试。从7个可用的支付系统中选择任何一个，点击 “生成卡” 并获得假的详细资料。

复制它们并将其粘贴在网站上，这样就不会从您的真实卡中扣钱。

这里的卡是虚构的，它当然不起作用。因此，如果您选择的服务要求您至少支付一分钱，那就无法使用它了。但对于免费注册直到付款的服务，卡片生成器是相当合适的。

 https://cardgenerator.org/

[image]
[image]

生成假的信用卡资料使注册更安全

[image] 关键词	个人 免追踪 数字足迹
[image] 创建时间	2022年5月11日
[image] **Description**	工具

信用卡生成器服务 Credit Card Generator 也许可以试试。从7个可用的支付系统中选择任何一个，点击 “生成卡” 并获得假的详细资料。

复制它们并将其粘贴在网站上，这样就不会从您的真实卡中扣钱。

这里的卡是虚构的，它当然不起作用。因此，如果您选择的服务要求您至少支付一分钱，那就无法使用它了。但对于免费注册直到付款的服务，卡片生成器是相当合适的。

 https://cardgenerator.org/

[image]
[image]

制作自己的二维码

[image] 关键词	QR码 倡导活动
[image] 创建时间	2022/05/13
[image] **Description**	工具

使用 QR-code-generator 服务，它可以对链接、文本、图像进行编码，有多种不同的选项。

您只需要插入您的信息，点击生成就可以下载一个QR码。

 https://www.qr-code-generator.com/

[image]
[image]

制作自己的二维码

[image] 关键词	QR码 倡导活动
[image] 创建时间	2022年5月13日
[image] **Description**	工具

使用 QR-code-generator 服务，它可以对链接、文本、图像进行编码，有多种不同的选项。

您只需要插入您的信息，点击生成就可以下载一个QR码。

 https://www.qr-code-generator.com/

[image]
[image]

巧妙地隐藏照片和视频

[image]	关键词	个人 反侦察 移动设备 防御
[image]	创建时间	2022年5月14日
[image]	**Description**	工具

您可以使用安卓版的 Photo Vault Calculator 应用程序或iOS版的Calculator# 来实现巧妙地隐藏敏感照片和视频 —— 它们可以用在很多方面：从简单的保护个人照片不被窥视，到隐藏重要文件（如果您只有手机没有电脑的话），例如，当智能手机在街边被警察强行搜查、或被海关人员检查时。

比如iOS：

1. 从 App Store下载该应用程序。
2. 进入其中，选择 "计算器"。
3. 输入密码，点击"%"。
4. 选择您想隐藏的文件类型。
5. 导入文件。

就可以了。

对于安卓版的该工具，它有闯入警报功能，不用担心有人尝试闯入。您还可以为这个假空间设置密码，即便它被人发现，也能避免危险。通过**AES**军事级加密算法，对那些您不想与人分享的内容进行加密，且对文件格式、大小没有任何限制；还支持直接拍照和录制私密视频。

对于iOS版，可密码保护隐藏的文档和其他文件；锁定音频以安全地记录语音笔记。可以从 PC、Mac 或其他设备进行 WiFi 传输。还有内置的 Web 浏览器、内置的密码管理器和钱包，内置安全笔记、待办事项和提醒，内置的联系人管理器。适用于 iPhone 和 iPad，两者都有 GUI。

 https://play.google.com/store/apps/details?id=com.hld.anzenbokusucal

 https://apps.apple.com/gb/app/calculator-hide-photos-videos/id1165276801

[image]
[image]

巧妙地隐藏照片和视频

[image]	关键词	个人 反侦察 移动设备 防御
[image]	创建时间	2022/05/14
[image]	**Description**	工具

您可以使用安卓版的 Photo Vault Calculator 应用程序或iOS版的Calculator# 来实现巧妙地隐藏敏感照片和视频 —— 它们可以用在很多方面：从简单的保护个人照片不被窥视，到隐藏重要文件（如果您只有手机没有电脑的话），例如，当智能手机在街边被警察强行搜查、或被海关人员检查时。

比如iOS：

1. 从 App Store下载该应用程序。
2. 进入其中，选择 "计算器"。
3. 输入密码，点击"%"。
4. 选择您想隐藏的文件类型。
5. 导入文件。

就可以了。

对于安卓版的该工具，它有闯入警报功能，不用担心有人尝试闯入。您还可以为这个假空间设置密码，即便它被人发现，也能避免危险。通过**AES**军事级加密算法，对那些您不想与人分享的内容进行加密，且对文件格式、大小没有任何限制；还支持直接拍照和录制私密视频。

对于iOS版，可密码保护隐藏的文档和其他文件；锁定音频以安全地记录语音笔记。可以从 PC、Mac 或其他设备进行 WiFi 传输。还有内置的 Web 浏览器、内置的密码管理器和钱包，内置安全笔记、待办事项和提醒，内置的联系人管理器。适用于 iPhone 和 iPad，两者都有 GUI。

 https://play.google.com/store/apps/details?id=com.hld.anzenbokusucal

 https://apps.apple.com/gb/app/calculator-hide-photos-videos/id1165276801

[image]
[image]

保密工具：找出是谁把您的文件或照片上传到了网络

[image] 关键词	反间谍 透明水印 防御 预防性
[image] 创建时间	2022年5月15日
[image] **Description**	工具

LeaksID 是一项允许您用隐形标签标记机密文件的服务。LeaksID 标记无法在没有该工具的情况下被检测到或移除。

工作方式：

1. 通过注册，上传重要文件，该网站将用隐形追踪器标记它们。
2. 然后，您将该服务创建的带有标记的副本发送给可疑的网站或个人。

就算接收者对您的文件进行截图，将其发送给第三方，甚至只是打印出来，LeaksID 都能够识别泄漏的来源并通知您。

https://leaksid.com/

[image]
[image]

保密工具：找出是谁把您的文件或照片上传到了网络

[image] 关键词	反间谍 透明水印 防御 预防性
[image] 创建时间	2022/05/15
[image] **Description**	工具

LeaksID 是一项允许您用隐形标签标记机密文件的服务。LeaksID 标记无法在没有该工具的情况下被检测到或移除。

工作方式：

1. 通过注册，上传重要文件，该网站将用隐形追踪器标记它们。
2. 然后，您将该服务创建的带有标记的副本发送给可疑的网站或个人。

就算接收者对您的文件进行截图，将其发送给第三方，甚至只是打印出来，LeaksID 都能够识别泄漏的来源并通知您。

https://leaksid.com/

[image]
[image]

在没有VPN的情况下访问被屏蔽的网站

[image] 关键词		反封锁
[image] 创建时间		2022/05/16
[image] **Description**		工具

CroxyProxy 是一款免费的代理服务，只需进入主页，并输入所需网站的链接。就行了。

无需注册，无需下载，无需验证。

 https://www.croxyproxy.com/

[image]
[image]

在没有VPN的情况下访问被屏蔽的网站

[image] 关键词	反封锁
[image] 创建时间	2022年5月16日
[image] **Description**	工具

CroxyProxy 是一款免费的代理服务，只需进入主页，并输入所需网站的链接。就行了。

无需注册，无需下载，无需验证。

 https://www.croxyproxy.com/

[image]
[image]

断网后通信：把智能手机变成“对讲机”

[image] 关键词		IMs 反封锁
[image] 创建时间		2022/05/18
[image] **Description**		工具

每当群体事件出现时您最先应该考虑到的就是断网。保持在断网情况下继续通信的能力非常重要。这方面的工具正在变得越来越多。

Two Way，不仅仅是一个离线通信工具，其工作方式就像一个对讲机。您和一个朋友（或一群朋友）选择一个频道号，然后就可以开始交谈。很简单，很方便，也很省事。

不需要注册，不会收集任何个人信息。

您可以使用地图选择频道号或位置，并与同一频道中的任何人交谈。它支持以最少的电池使用量在后台运行。

 https://play.google.com/store/apps/details?id=com.selvaraj.twoway.android

[image]
[image]

断网后通信：把智能手机变成“对讲机”

[image] 关键词	IMs 反封锁
[image] 创建时间	2022年5月18日
[image] **Description**	工具

每当群体事件出现时您最先应该考虑到的就是断网。保持在断网情况下继续通信的能力非常重要。这方面的工具正在变得越来越多。

Two Way，不仅仅是一个离线通信工具，其工作方式就像一个对讲机。您和一个朋友（或一群朋友）选择一个频道号，然后就可以开始交谈。很简单，很方便，也很省事。

不需要注册，不会收集任何个人信息。

您可以使用地图选择频道号或位置，并与同一频道中的任何人交谈。它支持以最少的电池使用量在后台运行。

 https://play.google.com/store/apps/details?id=com.selvaraj.twoway.android

[image]
[image]

彻底卸载

[image]	关键词	清理 电脑
[image]	创建时间	2022年5月20日
[image]	**Description**	工具

任何程序都会使电脑充满某种数据：注册表项、创建的文件夹、文件等。如果您只是简单地卸载一个应用程序，这些垃圾仍然会留在您的系统中，占用磁盘空间并影响性能。因此，建议使用专门的软件来卸载应用程序。

BCUninstaller 是一个强大的软件卸载程序，它可以在删除您电脑上的任何应用程序的同时清除任何痕迹或残留物。

 https://www.bcuninstaller.com/

[image]
[image]

彻底卸载

[image] 关键词	清理 电脑
[image] 创建时间	2022/05/20
[image] **Description**	工具

任何程序都会使电脑充满某种数据：注册表项、创建的文件夹、文件等。如果您只是简单地卸载一个应用程序，这些垃圾仍然会留在您的系统中，占用磁盘空间并影响性能。因此，建议使用专门的软件来卸载应用程序。

BCUninstaller 是一个强大的软件卸载程序，它可以在删除您电脑上的任何应用程序的同时清除任何痕迹或残留物。

 https://www.bcuninstaller.com/

[image]
[image]

在线防病毒扫描器

[image]	关键词	病毒检测 自检
[image]	创建时间	2022年5月21日
[image]	**Description**	工具

MetaDefender Cloud 是一个很好的在线防病毒扫描器，可以扫描文件、链接、IP地址、域名和哈希。除了识别可能的威胁外，它还扫描文件元数据和请求的权限。

进入网站，选择您需要的选项，并上传一个不超过140MB的文件。一旦启动，它将开始对数据进行全面分析，并生成一份详细报告。

 https://metadefender.opswat.com/

[image]
[image]

在线防病毒扫描器

[image] 关键词		病毒检测 自检
[image] 创建时间		2022/05/21
[image] **Description**		工具

MetaDefender Cloud 是一个很好的在线防病毒扫描器，可以扫描文件、链接、IP地址、域名和哈希。除了识别可能的威胁外，它还扫描文件元数据和请求的权限。

进入网站，选择您需要的选项，并上传一个不超过140MB的文件。一旦启动，它将开始对数据进行全面分析，并生成一份详细报告。

 https://metadefender.opswat.com/

[image]
[image]

假联系人 - 保护手机通讯录

[image]	关键词	免追踪 对抗性思考方式 移动设备 预防性
[image]	创建时间	2022年5月30日
[image]	**Description**	工具

几乎每一个移动应用程序都为老大哥服务。其中通讯录数据也是非常敏感的数据源之一，它可以勾勒您的人际关系网络，这是渗透操纵的入口。

Fake Contacts 是一个为联系人创建虚假数据的应用程序。也就是说它可以让无良公司收集到虚假的信息。与此同时您可以保留自己的真实联系人信息。

该应用程序是开源的，可以在 GitHub 上查看。

 https://f-droid.org/en/packages/me.billdietrich.fake_contacts/

 https://github.com/BillDietrich/fake_contacts

[image]
[image]

假联系人 - 保护手机通讯录

[image] 关键词	免追踪 对抗性思考方式 移动设备 预防性
[image] 创建时间	2022/05/30
[image] **Description**	工具

几乎每一个移动应用程序都为老大哥服务。其中通讯录数据也是非常敏感的数据源之一，它可以勾勒您的人际关系网络，这是渗透操纵的入口。

Fake Contacts 是一个为联系人创建虚假数据的应用程序。也就是说它可以让无良公司收集到虚假的信息。与此同时您可以保留自己的真实联系人信息。

该应用程序是开源的，可以在 GitHub 上查看。

 https://f-droid.org/en/packages/me.billdietrich.fake_contacts/

 https://github.com/BillDietrich/fake_contacts

[image]
[image]

绕开审查的浏览器

[image]	关键词	反封锁
[image]	创建时间	2022年5月31日
[image]	**Description**	工具

CENO是一个基于 Mozilla Firefox 的安卓手机网络浏览器，它将静态内容缓存在分布式网络中，通过中间临时节点（网桥）路由流量来规避审查。

当用户启动CENO浏览器时，他们将自动成为CENO网络的一部分。这意味着，在可能的情况下，这些设备应充当无法访问被阻止网站的人的临时VPN。

任何CENO用户访问的任何公共可用内容都以类似 BitTorrent 的方式与他人共享。

当用户打开一个网站时，下载的内容会被缓存在用户的系统中，并被不能直接访问该资源的P2P网络成员使用。每个设备上只存储从该设备直接请求的数据。

CENO浏览器由Ouinet提供支持，Ouinet是一个开源库，使第三方开发者能够将CENO网络纳入其应用程序，实现点对点连接。

https://github.com/censorship-no/ceno-browser/releases

[image]
[image]

绕开审查的浏览器

[image] 关键词		反封锁
[image] 创建时间		2022/05/31
[image] **Description**		工具

CENO是一个基于 Mozilla Firefox 的安卓手机网络浏览器，它将静态内容缓存在分布式网络中，通过中间临时节点（网桥）路由流量来规避审查。

当用户启动CENO浏览器时，他们将自动成为CENO网络的一部分。这意味着，在可能的情况下，这些设备应充当无法访问被阻止网站的人的临时VPN。

任何CENO用户访问的任何公共可用内容都以类似 BitTorrent 的方式与他人共享。

当用户打开一个网站时，下载的内容会被缓存在用户的系统中，并被不能直接访问该资源的P2P网络成员使用。每个设备上只存储从该设备直接请求的数据。

CENO浏览器由Ouinet提供支持，Ouinet是一个开源库，使第三方开发者能够将CENO网络纳入其应用程序，实现点对点连接。

https://github.com/censorship-no/ceno-browser/releases

[image]
[image]

恢复被删除的文件

[image] 关键词	取证 数据丢失 电脑 自助 自检
[image] 创建时间	2022年6月5日
[image] **Description**	工具

EaseUS Data Recovery Wizard 可以帮您恢复被删除的文件。

下载它，选择丢失数据的位置并开始搜索。然后运行扫描来恢复数据。 之后，您应该可以选择您想要恢复的文件。

 https://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm?srsltid=AfmBOooRZoiluLyS5TTbdsdlj-MDAQPVSyCOPXpKEqQVjQYFMMn-UBkr

[image]
[image]

恢复被删除的文件

[image] 关键词	取证 数据丢失 电脑 自助 自检
[image] 创建时间	2022/06/05
[image] **Description**	工具

EaseUS Data Recovery Wizard 可以帮您恢复被删除的文件。

下载它，选择丢失数据的位置并开始搜索。然后运行扫描来恢复数据。 之后，您应该可以选择您想要恢复的文件。

 https://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm?srsltid=AfmBOooRZoiluLyS5TTbdsdlj-MDAQPVSyCOPXpKEqQVjQYFMMn-UBkr

[image]
[image]

从照片中获取元数据的工具

[image] 关键词	数字足迹 自检
[image] 创建时间	2022/06/08
[image] **Description**	工具

当您使用了清除元数据的工具后，可以使用以下这些工具检查清理效果。

FBMD (Facebook metadata)：https://getpmd.iptc.org/getiptcpmd.html
Metadata2go：https://www.metadata2go.com/
Exiftool：https://exiftool.org/
Jimpl：https://jimpl.com/
Pic2Map：https://www.pic2map.com/

[image]
[image]

从照片中获取元数据的工具

[image] 关键词	数字足迹 自检
[image] 创建时间	2022年6月8日
[image] **Description**	工具

当您使用了清除元数据的工具后，可以使用以下这些工具检查清理效果。

FBMD (Facebook metadata)：https://getpmd.iptc.org/getiptcpmd.html
Metadata2go：https://www.metadata2go.com/
Exiftool：https://exiftool.org/
Jimpl：https://jimpl.com/
Pic2Map：https://www.pic2map.com/

[image]
[image]

虚拟手机号和马甲邮箱隐藏真实信息

[image] 关键词	免追踪 数字足迹 自助
[image] 创建时间	2022年6月18日
[image] **Description**	工具

当您用与您的真实身份相关的电子邮件在任何网站上注册时，您的邮件地址很可能会被泄露给某些恶意的数据库。您会收到大量的垃圾邮件，在最坏的情况下，您的电子邮件会被黑掉。

Firefox Relay 是一个官方的 Firefox 扩展，可以隐藏您的真实电子邮件地址，不被人窥视。该插件创建了一个假的邮件地址，在您注册时使用。所有电子邮件都从这个假邮箱转发到您的真实电子邮件帐户中。

这样，您就不会暴露真实邮箱，它也不会被网站看到。您最多可以创建5个电子邮件地址，并可以在任何时候禁用它们。只要直接安装就可以了。

 https://relay.firefox.com/

[image]
[image]

虚拟手机号和马甲邮箱隐藏真实信息

[image] 关键词	免追踪 数字足迹 自助
[image] 创建时间	2022/06/18
[image] **Description**	工具

当您用与您的真实身份相关的电子邮件在任何网站上注册时，您的邮件地址很可能会被泄露给某些恶意的数据库。您会收到大量的垃圾邮件，在最坏的情况下，您的电子邮件会被黑掉。

Firefox Relay 是一个官方的 Firefox 扩展，可以隐藏您的真实电子邮件地址，不被人窥视。该插件创建了一个假的邮件地址，在您注册时使用。所有电子邮件都从这个假邮箱转发到您的真实电子邮件帐户中。

这样，您就不会暴露真实邮箱，它也不会被网站看到。您最多可以创建5个电子邮件地址，并可以在任何时候禁用它们。只要直接安装就可以了。

 https://relay.firefox.com/

[image]
[image]

匿名上传文件以在线分享

[image] 关键词	传输安全 免追踪
[image] 创建时间	2022/06/20
[image] **Description**	工具

您想分享一个不太大的文件吗？可以使用文件共享网站，但那些网站不能保证您的安全。

 anonfile.la - 这个网站允许您匿名和免费地上传高达20GB的文件。没有人为的速度限制。

根据开发者的说法，内容的链接将永远有效，虽然有一些例外。

上传的内容都可以在网站本身查看，没有任何问题。

[image]
[image]

匿名上传文件以在线分享

[image] 关键词	传输安全 免追踪
[image] 创建时间	2022年6月20日
[image] **Description**	工具

您想分享一个不太大的文件吗？可以使用文件共享网站，但那些网站不能保证您的安全。

 anonfile.la - 这个网站允许您匿名和免费地上传高达20GB的文件。没有人为的速度限制。

根据开发者的说法，内容的链接将永远有效，虽然有一些例外。

上传的内容都可以在网站本身查看，没有任何问题。

[image]
[image]

快速搭建自己的VPN服务

[image]	关键词	反封锁 自助
[image]	创建时间	2022/06/21
[image]	**Description**	工具

这个脚本可以让您在一分钟内建立自己的VPN服务器，新手也没问题。

它被设计成尽可能的不显眼和通用。

它可以在 Ubuntu, Debian, AlmaLinux , Rocky Linux, CentOS 和 Fedora 上运行。

 https://github.com/Nyr/wireguard-install

[image]
[image]

快速搭建自己的VPN服务

[image]	关键词	反封锁 自助
[image]	创建时间	2022年6月21日
[image]	**Description**	工具

这个脚本可以让您在一分钟内建立自己的VPN服务器，新手也没问题。

它被设计成尽可能的不显眼和通用。

它可以在 Ubuntu, Debian, AlmaLinux , Rocky Linux, CentOS 和 Fedora 上运行。

 https://github.com/Nyr/wireguard-install

[image]
[image]

检查一个应用程序是否有恶意代码

[image] 关键词	安卓 病毒检测 移动设备 自助
[image] 创建时间	2022/06/25
[image] **Description**	工具

在 “安卓还是iPhone” 的争论中，安卓粉丝经常争辩说，他们可以从任何地方安装任何应用程序，苹果就不行。虽然已经部分消除了这个神话，但不可否认的是，在安卓系统上从外部来源安装应用程序要容易得多，但也有很多风险。

Ostorlab 是一项用于识别移动应用程序中的漏洞和恶意代码的服务。它分析的威胁包括：嵌入式短信、密码劫持，以及对应用程序的个人数据要求过高等等。

使用很简单：点击 “新扫描”，选择一个应用商店/网站和应用名称，或上传您自己的应用，然后点击 “提交”。请注意，扫描需要一些时间，您足够喝一杯的。

 https://ostorlab.co/

[image]
[image]

检查一个应用程序是否有恶意代码

[image] 关键词	安卓 病毒检测 移动设备 自助
[image] 创建时间	2022年6月25日
[image] **Description**	工具

在 “安卓还是iPhone” 的争论中，安卓粉丝经常争辩说，他们可以从任何地方安装任何应用程序，苹果就不行。虽然已经部分消除了这个神话，但不可否认的是，在安卓系统上从外部来源安装应用程序要容易得多，但也有很多风险。

Ostorlab 是一项用于识别移动应用程序中的漏洞和恶意代码的服务。它分析的威胁包括：嵌入式短信、密码劫持，以及对应用程序的个人数据要求过高等等。

使用很简单：点击 “新扫描”，选择一个应用商店/网站和应用名称，或上传您自己的应用，然后点击 “提交”。请注意，扫描需要一些时间，您足够喝一杯的。

 https://ostorlab.co/

[image]
[image]

读取陌生的/不受信任的USB设备

[image] 关键词 威胁识别 电脑 自检

[image] 创建时间 2022/06/28

[image] **Description** 工具

如果您有一个USB设备，但是您不知道它是否可信，并且对其中有什么东西好奇。千万不要把它直接插入您的电脑，您需要一个工具，一个能够安全读取不受信任的USB存储设备的工具。

usbsas 就是这样一个工具。它可以：

- 从USB设备上读取文件，不需要使用 uas、usb_storage 和文件系统等内核模块；
- 通过远程反病毒手段进行文件分析；
- 将文件复制到一个可信的USB设备上；
- 将文件上传到远程服务器；
- 创建镜像；
- 清理USB设备。

 https://github.com/cea-sec/usbsas

[image]
[image]

读取陌生的/不受信任的USB设备

[image]	关键词	威胁识别 电脑 自检
[image]	创建时间	2022年6月28日
[image]	**Description**	工具

如果您有一个USB设备，但是您不知道它是否可信，并且对其中有什么东西好奇。千万不要把它直接插入您的电脑，您需要一个工具，一个能够安全读取不受信任的USB存储设备的工具。

usbsas 就是这样一个工具。它可以：

- 从USB设备上读取文件，不需要使用 uas、usb_storage 和文件系统等内核模块；
- 通过远程反病毒手段进行文件分析；
- 将文件复制到一个可信的USB设备上；
- 将文件上传到远程服务器；
- 创建镜像；
- 清理USB设备。

 https://github.com/cea-sec/usbsas

[image]
[image]

安全的保存您想要的链接

[image] 关键词	效率 查询整理 电脑
[image] 创建时间	2022年6月29日
[image] **Description**	工具

LinkWarden 是一个独立的、开源的书签和文档管理器，可以收集和保存网站，并在离线时使用。

目的是让您有自己的地方来储存有用的链接。由于有用的链接可能会消失，LinkWarden 也会将链接的副本保存为屏幕截图和PDF。

▫支持暗模式。
▫响应式设计。
▫搜索、过滤和排序功能。
以及更多...

 https://github.com/Daniel31x13/link-warden

[image]
[image]

安全的保存您想要的链接

[image] 关键词	效率 查询整理 电脑
[image] 创建时间	2022/06/29
[image] **Description**	工具

LinkWarden 是一个独立的、开源的书签和文档管理器，可以收集和保存网站，并在离线时使用。

目的是让您有自己的地方来储存有用的链接。由于有用的链接可能会消失，LinkWarden 也会将链接的副本保存为屏幕截图和PDF。

▫支持暗模式。
▫响应式设计。
▫搜索、过滤和排序功能。
以及更多...

 https://github.com/Daniel31x13/link-warden

[image]
[image]

简易P2P信使

[image] 关键词	IMs P2P 加密
[image] 创建时间	2022年7月14日
[image] **Description**	工具

Communist 是一个基于GTK 4 的简单p2p 通信工具。

它使用分布式哈希表（DHT torrent）和UDP打洞方法相结合，在用户之间建立直接连接。

它可以在两种模式下运行：局域网和互联网。
▫支持IPv4和IPv6。
▫可以发送简单的文本信息和文件。
▫您的所有信息和文件都是加密存储和加密发送的。

 https://github.com/ProfessorNavigator/communist

[image]
[image]

简易P2P信使

[image] 关键词	IMs P2P 加密
[image] 创建时间	2022/07/14
[image] **Description**	工具

Communist 是一个基于GTK 4 的简单p2p 通信工具。

它使用分布式哈希表（DHT torrent）和UDP打洞方法相结合，在用户之间建立直接连接。

它可以在两种模式下运行：局域网和互联网。
▫支持IPv4和IPv6。
▫可以发送简单的文本信息和文件。
▫您的所有信息和文件都是加密存储和加密发送的。

 https://github.com/ProfessorNavigator/communist

[image]
[image]

没有审查的多媒体内容管理系统

[image] 关键词	反审查 自托管
[image] 创建时间	2022/07/17
[image] **Description**	工具

MediaCMS是一个全功能的、开源的视频和多媒体CMS。

它可以用来在几分钟内创建您自己的中小型视频和媒体门户。

它的私密性适合那种难以上传到外部站点的敏感内容。

特点：

自托管：您完全控制自己的数据；
多种媒体类型支持：视频、音频、图像、pdf；
多种媒体分享选项：社交媒体分享、视频嵌入代码生成；
Subtitles/CC：支持多语种字幕文件

https://github.com/mediacms-io/mediacms

[image]
[image]

没有审查的多媒体内容管理系统

[image] 关键词	反审查 自托管
[image] 创建时间	2022年7月17日
[image] **Description**	工具

MediaCMS是一个全功能的、开源的视频和多媒体CMS。

它可以用来在几分钟内创建您自己的中小型视频和媒体门户。

它的私密性适合那种难以上传到外部站点的敏感内容。

特点：

自托管：您完全控制自己的数据；
多种媒体类型支持：视频、音频、图像、pdf；
多种媒体分享选项：社交媒体分享、视频嵌入代码生成；
Subtitles/CC：支持多语种字幕文件

https://github.com/mediacms-io/mediacms

[image]
[image]

免费的macOS清洁软件

[image] 关键词		清理 电脑
[image] 创建时间		2022/07/19
[image] **Description**		工具

许多macOS用户都听说过CleanMyMac。它非常善于清除系统中不必要的垃圾和卸载应用程序的残余文件。然而，它并不便宜，而且盗版也不是最佳选择。

还有其他工具可以清理你的系统，AppCleaner就是其中之一。一个清理macOS的免费程序，它非常简单，只需将应用程序拖放到AppCleaner 窗口中即可，它会给你一个列表，你所要做的就是选择你想删除的东西。

AppCleaner - 没有CleanMyMac那么多功能，但它是免费的。它能够从系统中删除不必要的垃圾，这正是许多用户所需要的。

 https://freemacsoft.net/appcleaner/

[image]
[image]

免费的macOS清洁软件

[image] 关键词	清理 电脑
[image] 创建时间	2022年7月19日
[image] **Description**	工具

许多macOS用户都听说过CleanMyMac。它非常善于清除系统中不必要的垃圾和卸载应用程序的残余文件。然而，它并不便宜，而且盗版也不是最佳选择。

还有其他工具可以清理你的系统，AppCleaner就是其中之一。一个清理macOS的免费程序，它非常简单，只需将应用程序拖放到AppCleaner 窗口中即可，它会给你一个列表，你所要做的就是选择你想删除的东西。

AppCleaner - 没有CleanMyMac那么多功能，但它是免费的。它能够从系统中删除不必要的垃圾，这正是许多用户所需要的。

 https://freemacsoft.net/appcleaner/

[image]
[image]

检查您的密码是否被泄漏了

[image]	关键词	密码 自检 预防性
[image]	创建时间	2022年7月20日
[image]	**Description**	工具

以下这些都可以：

- 🖇 have i been pwned：https://haveibeenpwned.com/
- 🖇 DeHashed：https://www.dehashed.com
- 🖇 Leakcheck：https://leakcheck.io
- 🖇 Firefox monitor：https://monitor.mozilla.org/
- 🖇 Spy Cloud：https://spycloud.com/check-your-exposure/

使用这些服务很容易，只要输入您需要检查的私人信息，看看您的数据是否被泄露。如果有，迅速更改密码。

[image]
[image]

检查您的密码是否被泄漏了

[image] 关键词	密码 自检 预防性
[image] 创建时间	2022/07/20
[image] **Description**	工具

以下这些都可以：

- have i been pwned：https://haveibeenpwned.com/
- DeHashed：https://www.dehashed.com
- Leakcheck：https://leakcheck.io
- Firefox monitor：https://monitor.mozilla.org/
- Spy Cloud：https://spycloud.com/check-your-exposure/

使用这些服务很容易，只要输入您需要检查的私人信息，看看您的数据是否被泄露。如果有，迅速更改密码。

[image]
[image]

对您的电脑上的文件夹进行加密

[image] 关键词	加密 文件处理 电脑
[image] 创建时间	2022年7月21日
[image] **Description**	工具

重要文件、个人数据、密码 —— 每个人都有需要保留在电脑上的重要东西。但 Windows 和 Mac OS 密码并不能提供100%的保护和安全。最简单的方法是在文件夹和特定文件上设置密码。

Anvi Folder Locker 是一个可以在文件夹上设置密码或隐藏文件夹的程序，使其他人无法找到它。

使用很简单，您只需要：

1. 安装该程序。

1. 编一个密码输入。

1. 指定电子邮件。

1. 选择一个文件夹，就完成了。

 wins：https://anvi-folder-locker-free.en.download.it/

 Mac：https://apps.apple.com/app/folder-lock/id1498304829

[image]
[image]

对您的电脑上的文件夹进行加密

[image] 关键词	加密 文件处理 电脑
[image] 创建时间	2022/07/21
[image] **Description**	工具

重要文件、个人数据、密码 —— 每个人都有需要保留在电脑上的重要东西。但 Windows 和 Mac OS 密码并不能提供100%的保护和安全。最简单的方法是在文件夹和特定文件上设置密码。

Anvi Folder Locker 是一个可以在文件夹上设置密码或隐藏文件夹的程序，使其他人无法找到它。

使用很简单，您只需要：

1. 安装该程序。

1. 编一个密码输入。

1. 指定电子邮件。

1. 选择一个文件夹，就完成了。

 wins：https://anvi-folder-locker-free.en.download.it/

 Mac：https://apps.apple.com/app/folder-lock/id1498304829

[image]
[image]

隐私导向的YouTube界面

[image]	关键词	免追踪 反审查
[image]	创建时间	2022/07/26
[image]	**Description**	工具

Piped：一个替代性的、隐私安全的YouTube界面。

- 没有广告
- 没有跟踪
- 方便使用
- 无限滚动
- 浅色/暗色主题
- 播放列表
- 与SponsorBlock整合
- 支持4K
- 没有连接到谷歌服务器

- 只播放音频模式
- 支持PWA
- 对iOS的支持
- 本地保存的设置

 https://github.com/TeamPiped/Piped

[image]
[image]

隐私导向的YouTube界面

[image]	关键词	免追踪 反审查
[image]	创建时间	2022年7月26日
[image]	**Description**	工具

Piped：一个替代性的、隐私安全的YouTube界面。

- 没有广告
- 没有跟踪
- 方便使用
- 无限滚动
- 浅色/暗色主题
- 播放列表
- 与SponsorBlock整合
- 支持4K
- 没有连接到谷歌服务器

- 只播放音频模式
- 支持PWA
- 对iOS的支持
- 本地保存的设置

 https://github.com/TeamPiped/Piped

[image]
[image]

方便的隐私套件

[image] 关键词		免追踪 自助
[image] 创建时间		2022年7月27日
[image] **Description**		工具

如果您不想为了匿名和隐私保护而下载一大堆的程序，可以考虑使用 SeaMonkey。

SeaMonkey 是一个工作和匿名软件的宝库。它有一个电子邮件客户端，一个易于使用的网络浏览器，一个名为 ChatZilla 的IRC客户端，和为开发者提供的工具。完全可以满足日常隐私保护的需求。

您可以在任何操作系统上安装它。

 https://www.seamonkey-project.org/

[image]
[image]

方便的隐私套件

[image]	关键词	免追踪 自助
[image]	创建时间	2022/07/27
[image]	**Description**	工具

如果您不想为了匿名和隐私保护而下载一大堆的程序，可以考虑使用SeaMonkey。

SeaMonkey 是一个工作和匿名软件的宝库。它有一个电子邮件客户端，一个易于使用的网络浏览器，一个名为 ChatZilla 的IRC客户端，和为开发者提供的工具。完全可以满足日常隐私保护的需求。

您可以在任何操作系统上安装它。

 https://www.seamonkey-project.org/

[image]
[image]

在没有数字足迹的情况下发送秘密信息

[image] 关键词	传输安全 免追踪 加密 数字足迹
[image] 创建时间	2022年8月2日
[image] **Description**	工具

当您需要与另一个人分享重要的数据，如密码和护照信息时，如果通过端对端加密的即时通信工具或邮件发送，请记得接收后立刻删除。如果您忘记删除了 —— 当账户被入侵时，黑客将拥有这些数据。

但有些时候您可能因为无法翻墙而无法使用安全的通信工具。那么，

Sendsecure.ly - 这项服务通过创建一个内含秘密信息的一次性链接，使信息传递的安全性提高了很多。您可以以一种方便的方式将其发送给合适的人。

一旦被打开，或在一段时间后，该链接将失效，以便只有您的联系人可以使用您提供的数据。您还可以自行设置链接在几分钟后过期。

一切都是加密的，服务的开发者无法看到您所分享的内容。

 https://sendsecure.ly/

[image]
[image]

在没有数字足迹的情况下发送秘密信息

[image] 关键词	传输安全 免追踪 加密 数字足迹
[image] 创建时间	2022/08/02
[image] **Description**	工具

当您需要与另一个人分享重要的数据，如密码和护照信息时，如果通过端对端加密的即时通信工具或邮件发送，请记得接收后立刻删除。如果您忘记删除了 —— 当账户被入侵时，黑客将拥有这些数据。

但有些时候您可能因为无法翻墙而无法使用安全的通信工具。那么，

Sendsecure.ly - 这项服务通过创建一个内含秘密信息的一次性链接，使信息传递的安全性提高了很多。您可以以一种方便的方式将其发送给合适的人。

一旦被打开，或在一段时间后，该链接将失效，以便只有您的联系人可以使用您提供的数据。您还可以自行设置链接在几分钟后过期。

一切都是加密的，服务的开发者无法看到您所分享的内容。

 https://sendsecure.ly/

[image]
[image]

快速检查可疑程序

[image]	关键词	病毒检测 自助
[image]	创建时间	2022年8月3日
[image]	**Description**	工具

Hybrid Analysis - 是一项免费的服务，提供了一个可能比杀毒软件更可靠和快捷的方法来检查可能的恶意程序。它对可疑文件进行 “试运行”，在提交文件进行检查后，它在一个隔离的 VirtualBox 或 VMware 沙箱中运行，然后观察它在系统上的表现。

如果它感染了一个虚拟机，该服务将在摘要中建议不要安装它。

 https://www.hybrid-analysis.com/

[image]
[image]

快速检查可疑程序

[image] 关键词	病毒检测 自助
[image] 创建时间	2022/08/03
[image] **Description**	工具

Hybrid Analysis - 是一项免费的服务，提供了一个可能比杀毒软件更可靠和快捷的方法来检查可能的恶意程序。它对可疑文件进行 “试运行”，在提交文件进行检查后，它在一个隔离的 VirtualBox 或 VMware 沙箱中运行，然后观察它在系统上的表现。

如果它感染了一个虚拟机，该服务将在摘要中建议不要安装它。

 https://www.hybrid-analysis.com/

[image]
[image]

加强电子设备防盗水平

[image] 关键词	反侦察 数据丢失 电脑 移动设备 预防性
[image] 创建时间	2022/08/06
[image] **Description**	工具

如果您的智能手机或笔记本电脑被盗，不要指望警察，那很可能没用（还没准儿就是他们偷的呢）。最好是让您可以远程控制自己的电脑或手机。

Prey 是一个设备追踪平台，在它的帮助下，您可以远程删除所有数据、检索或加密数据，以及从被盗或丢失的设备的摄像头拍摄快照。

还有其他优点：当设备在特定区域时，软件可以提醒您，并且有一个位置的历史记录，每小时更新一次。主要的前提条件是互联网连接，不需要GPS。

 https://preyproject.com/

[image]
[image]

加强电子设备防盗水平

[image] 关键词	反侦察 数据丢失 电脑 移动设备 预防性
[image] 创建时间	2022年8月6日
[image] **Description**	工具

如果您的智能手机或笔记本电脑被盗，不要指望警察，那很可能没用（还没准儿就是他们偷的呢）。最好是让您可以远程控制自己的电脑或手机。

Prey 是一个设备追踪平台，在它的帮助下，您可以远程删除所有数据、检索或加密数据，以及从被盗或丢失的设备的摄像头拍摄快照。

还有其他优点：当设备在特定区域时，软件可以提醒您，并且有一个位置的历史记录，每小时更新一次。主要的前提条件是互联网连接，不需要GPS。

 https://preyproject.com/

[image]
[image]

在断网的情况下保持联系

[image] 关键词	传输安全 反封锁 移动设备 预防性
[image] 创建时间	2022/08/13
[image] **Description**	工具

如您所知，全世界的统治者都擅长用切断互联网来维稳，前段时间中国郑州的抗议现场出现的信号屏蔽车并不是什么特殊现象，而是标准做法。

IYP有一个“如何应对断网”专栏，但其中的内容大多是为活动家服务的，保护他们尽可能在断网的情况下也可以继续工作。

断网情况下最常见的需求可能的通信，于是这些年来，不依赖互联网的通信技术获得了更多的重视。比如很早以前流行过一段时间的 Firechat（已经不更新了），以及后来的 Bridgefy（依赖谷歌服务，中国不方便使用）。

简单说，这类即时通信工具使用您的Wi-Fi或蓝牙来联系周边其他人。

此外还有一个：Signal Offline Messenger，也是一个离线消息应用程序。 允许您在不超过 100 米的范围内无需互联网或本地网络而进行通信。用户可以通过 Wi-Fi Direct 向附近的其他用户分享音频、文本、照片和视频消息。 支持三种方案：Android、iPhone 和 Online/Web。

类似的还有 Talkie，也是一个在没有互联网或蜂窝网络的情况下进行

通信的工具，支持语音通话，以 Wi-Fi 速度传输文件和文件夹，可私聊也可以群聊。它承诺即使 Wi-Fi 信号非常微弱，音质也很好；支持蓝牙耳机，免提模式等。

[image]
[image]

在断网的情况下保持联系

[image] 关键词 传输安全 反封锁 移动设备 预防性

[image] 创建时间 2022年8月13日

[image] **Description** 工具

如您所知，全世界的统治者都擅长用切断互联网来维稳，前段时间中国郑州的抗议现场出现的信号屏蔽车并不是什么特殊现象，而是标准做法。

IYP有一个“如何应对断网”专栏，但其中的内容大多是为活动家服务的，保护他们尽可能在断网的情况下也可以继续工作。

断网情况下最常见的需求可能的通信，于是这些年来，不依赖互联网的通信技术获得了更多的重视。比如很早以前流行过一段时间的 Firechat（已经不更新了），以及后来的 Bridgefy（依赖谷歌服务，中国不方便使用）。

简单说，这类即时通信工具使用您的Wi-Fi或蓝牙来联系周边其他人。

此外还有一个：Signal Offline Messenger，也是一个离线消息应用程序。 允许您在不超过 100 米的范围内无需互联网或本地网络而进行通信。用户可以通过 Wi-Fi Direct 向附近的其他用户分享音频、文本、照片和视频消息。 支持三种方案：Android、iPhone 和 Online/Web。

类似的还有 Talkie，也是一个在没有互联网或蜂窝网络的情况下进行

通信的工具，支持语音通话，以 Wi-Fi 速度传输文件和文件夹，可私聊也可以群聊。它承诺即使 Wi-Fi 信号非常微弱，音质也很好；支持蓝牙耳机，免提模式等。

[image]
[image]

如果你被迫解锁手机，应该怎么做

[image] 关键词	反审查 反间谍 密码 自助 预防性
[image] 创建时间	2022/08/19
[image] Description	工具

想象一下，如果你被警察抓到，而你的手机上有警察不应该看到的数据（他们不应该看到一切）。

Duress 是一个允许你生成无效密码的应用程序，一旦输入该密码，它将向你指定的亲人/队友发送通知。你也可以用这个假密码来擦除你想隐藏的敏感数据。

攻击者甚至不会注意到。正常的密码仍然有效，如果你输入密码，设备就会被解锁。

当然希望你不要陷入这种情况，尤其是，尽可能不要在手机上保留那种非常重要的信息。

 https://play.google.com/store/apps/details?id=me.lucky.duress

[image]
[image]

如果您的手机被盗了或被警察抢走了，怎么办

[image] 关键词	免追踪 反间谍 数据丢失 移动设备 自助 预防性
[image] 关联	[image]注重隐私的智能手机
[image] 创建时间	2022年8月19日
[image] Description	工具

这个小指南也许可以防止今后出现不愉快的情况。

iPhone 的拥有者在这方面要容易一些，安全措施很简单。打开设置，进入 “面部识别和密码”，打开 “清除数据”。在十次密码尝试不成功后，iPhone 将删除所有数据。

对于安卓用户来说，Google Play上有3个不错的应用程序：

 Duress - 它为用户可能被警察强迫解锁手机的危险情况而创建。在这个应用程序中，可以设置一个假密码，当输入后，用户的亲人会得到相应的通知。

 Lookwatch — 每次有人试图解锁您的手机不成功时，都会在前置摄像头上拍照，并发送到您指定的邮箱里。您就会知道是谁在试图解锁您的手机。

 Wasted - 在紧急情况下完全锁定和擦除您的手机。例如，如果设备已经几天没有开机了。

[image]

返回：[image]如果您的手机被盗或被警察抢走...

返回：[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？

返回：[image]如何保持 Android 设备免受警察的侵害

[image]
[image]

如果你被迫解锁手机，应该怎么做

[image] 关键词	反审查 反间谍 密码 自助 预防性
[image] 创建时间	2022年8月19日
[image] **Description**	工具

想象一下，如果你被警察抓到，而你的手机上有警察不应该看到的数据（他们不应该看到一切）。

Duress 是一个允许你生成无效密码的应用程序，一旦输入该密码，它将向你指定的亲人/队友发送通知。你也可以用这个假密码来擦除你想隐藏的敏感数据。

攻击者甚至不会注意到。正常的密码仍然有效，如果你输入密码，设备就会被解锁。

当然希望你不要陷入这种情况，尤其是，尽可能不要在手机上保留那种非常重要的信息。

 https://play.google.com/store/apps/details?id=me.lucky.duress

[image]
[image]

如果您的手机被盗了或被警察抢走了，怎么办

[image] 关键词	免追踪 反间谍 数据丢失 移动设备 自助 预防性
[image] 创建时间	2022/08/19
[image] **Description**	工具

这个小指南也许可以防止今后出现不愉快的情况。

iPhone 的拥有者在这方面要容易一些，安全措施很简单。打开设置，进入 “面部识别和密码”，打开 “清除数据”。在十次密码尝试不成功后，iPhone 将删除所有数据。

对于安卓用户来说，Google Play上有3个不错的应用程序：

 Duress - 它为用户可能被警察强迫解锁手机的危险情况而创建。在这个应用程序中，可以设置一个假密码，当输入后，用户的亲人会得到相应的通知。

 Lookwatch — 每次有人试图解锁您的手机不成功时，都会在前置摄像头上拍照，并发送到您指定的邮箱里。您就会知道是谁在试图解锁您的手机。

 Wasted - 在紧急情况下完全锁定和擦除您的手机。例如，如果设备已经几天没有开机了。

📌 如果您错过了：
《如果您的手机被盗或被警察抢走...》
《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
《如何让您的 iPhone 能够防小偷》
《如何保持 Android 设备免受警察的侵害》

[image]
[image]

安卓恶意软件扫描器

[image] 关键词	安卓 病毒检测 移动设备 自助 自检
[image] 创建时间	2022/08/20
[image] **Description**	工具

Hypatia - 这是一个开源的Android恶意软件扫描器。它的工作原理是基于ClamAV式的签名数据库。

▫对电池的影响几乎为零
▫极快
▫定期扫描
▫联网只用于下载签名数据库，文件永远不会离开你的设备
▫当您下载/更新时自动重新启动
▫最小的依赖性
以及更多...

□ https://gitlab.com/divested-mobile/hypatia

□ F-droid: https://f-droid.org/en/packages/us.spotco.malwarescanner/

[image]
[image]

安卓恶意软件扫描器

[image] 关键词	安卓 病毒检测 移动设备 自助 自检
[image] 关联	恶意软件
[image] 创建时间	2022年8月20日
[image] **Description**	工具

Hypatia - 这是一个开源的Android恶意软件扫描器。它的工作原理是基于ClamAV式的签名数据库。

▫对电池的影响几乎为零
▫极快
▫定期扫描
▫联网只用于下载签名数据库，文件永远不会离开你的设备
▫当您下载/更新时自动重新启动
▫最小的依赖性
以及更多...

https://gitlab.com/divested-mobile/hypatia

F-droid: https://f-droid.org/en/packages/us.spotco.malwarescanner/

[image]
[image]

隐藏秘密信息

[image] 关键词	传输安全 移动设备 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2022年8月24日
[image] Description	工具

隐藏秘密信息的最简单方法就是把它们放在最显眼的地方。

老读者知道，我们介绍过很多隐写的方法，比如将秘密信息隐藏在图片中、隐藏在一首歌曲中、或者直接隐藏在完全不相关的文本中。这种方法很适合那种您不得不使用不安全的通信渠道（比如微信、推特等）传递敏感信息时的状况。

数字隐写术的相关工具几十年来一直在更新换代，但依旧需要一些使用技巧来绕过其弱点。

🖋 StegCloak - 这是一个较新的隐写工具，原理是一样的，即 使用隐形Unicode字符将数据隐藏在文本内。该软件使用AES-256-CTR加密，以尽可能的安全。

这项服务的使用范围很大：可用于论坛、隐形推文、各种社交媒体、不安全的即时消息应用等，或简单地隐藏所有数据。

您也可以使用这项服务来隐藏文件。但要做到这一点您必须将一个文件上传到云，获得一个链接然后将其隐藏在文本中。上传云之前一定要记得加密哦，您知道该使用什么加密工具。

有一点需要注意的是，当您知道有人在主动嗅探您的数据时 —— 也就是您在实名工作已经被重点监视的情况下，请不要使用隐写工具，因为通过数据分析工具就可以很简单地看到 unicode 字符。在那种情况下即使密码无法破译，隐写的基本功能也被破坏了 —— 隐写的功能是旨在隐藏“正在发送秘密通信”的事实。

换句话说，该方法无法解决 Alice-Bob-Warden 的问题。这也正是为什么我们建议著名敏感人士采取分身，让分身角色难以被追踪，以便绕开“Warden”。

 https://stegcloak.surge.sh/

[image]
[image]

隐藏秘密信息

[image] 关键词	传输安全 移动设备 隐写术
[image] 创建时间	2022/08/24
[image] Description	工具

隐藏秘密信息的最简单方法就是把它们放在最显眼的地方。

老读者知道，我们介绍过很多隐写的方法，比如将秘密信息隐藏在图片中、隐藏在一首歌曲中、或者直接隐藏在完全不相关的文本中。这种方法很适合那种您不得不使用不安全的通信渠道（比如微信、推特等）传递敏感信息时的状况。

数字隐写术的相关工具几十年来一直在更新换代，但依旧需要一些使用技巧来绕过其弱点。

🖇 StegCloak - 这是一个较新的隐写工具，原理是一样的，即 使用隐形Unicode字符将数据隐藏在文本内。该软件使用AES-256-CTR加密，以尽可能的安全。

这项服务的使用范围很大：可用于论坛、隐形推文、各种社交媒体、不安全的即时消息应用等，或简单地隐藏所有数据。

您也可以使用这项服务来隐藏文件。但要做到这一点您必须将一个文件上传到云，获得一个链接然后将其隐藏在文本中。上传云之前一定要记得加密哦，您知道该使用什么加密工具。

有一点需要注意的是，当您知道有人在主动嗅探您的数据时 —— 也就是您在实名工作已经被重点监视的情况下，请不要使用隐写工具，因为通过数据分析工具就可以很简单地看到 unicode 字符。在那种情况下即使密码无法破译，隐写的基本功能也被破坏了 —— 隐写的功能是旨在隐藏“正在发送秘密通信”的事实。

换句话说，该方法无法解决 Alice-Bob-Warden 的问题。这也正是为什么我们建议著名敏感人士采取分身，让分身角色难以被追踪，以便绕开“Warden”。

□ https://stegcloak.surge.sh/

[image]
[image]

快速构建一个假名账户

[image] 关键词	免追踪 反侦察 自助 预防性
[image] 创建时间	2022/08/25
[image] **Description**	工具

许多网站要求用户创建一个账户才能访问网站上的内容。如果您不想提供您的真实资料，那就需要一个假身份生成器。

Reggy - 是一个生成随机数据并自动插入注册表格的扩展。除了假身份外，该扩展还提供了一个电邮。所以您不必再使用一次性的电子邮件服务。

 https://chromewebstore.google.com/detail/reggy/pnneajlgffpejnabhionnhdfhibijihe?pli=1

[image]
[image]

快速构建一个假名账户

[image] 关键词	免追踪 反侦察 自助 预防性
[image] 创建时间	2022年8月25日
[image] **Description**	工具

许多网站要求用户创建一个账户才能访问网站上的内容。如果您不想提供您的真实资料，那就需要一个假身份生成器。

Reggy - 是一个生成随机数据并自动插入注册表格的扩展。除了假身份外，该扩展还提供了一个电邮。所以您不必再使用一次性的电子邮件服务。

 https://chromewebstore.google.com/detail/reggy/pnneajlgffpejnabhionnhdfhibijihe?pli=1

[image]
[image]

安全地存储文本(消息、登录凭据、密钥、笔记...)

[image] 关键词	传输安全 加密 反侦察 自助 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2022年8月26日
[image] **Description**	工具

在90%的情况下，最有价值的数据是文本数据。敏感信息、即时通信中的消息、登录凭据、笔记、密钥 —— 如果攻击者获得了这些数据，情况将非常糟糕。

Paranoia Text Encryption 是对这类敏感文本进行加密的服务。该程序使用最强的加密算法 —— Blowfish 448位，AES 256位，RC6 256位，Serpent 256位，Twofish 256位，GOST 256位。

使用很简单：

- 从您喜欢的任何应用程序中复制和粘贴数据，
- 把它保存到一个文件中，以便以后使用。
- 它还包括隐写术实践，把文本隐藏图像中(JPEG 图像)。
- 免费开源，广泛兼容。

您会找到有创意的用例。

 https://paranoiaworks.mobi/ptepc/

[image]
[image]

安全地存储文本(消息、登录凭据、密钥、笔记...)

[image] 关键词	传输安全 加密 反侦察 自助 隐写术
[image] 创建时间	2022/08/26
[image] **Description**	工具

在90%的情况下，最有价值的数据是文本数据。敏感信息、即时通信中的消息、登录凭据、笔记、密钥 —— 如果攻击者获得了这些数据，情况将非常糟糕。

Paranoia Text Encryption 是对这类敏感文本进行加密的服务。该程序使用最强的加密算法 —— Blowfish 448位，AES 256位，RC6 256位，Serpent 256位，Twofish 256位，GOST 256位。

使用很简单：

- 从您喜欢的任何应用程序中复制和粘贴数据，
- 把它保存到一个文件中，以便以后使用。
- 它还包括隐写术实践，把文本隐藏图像中(JPEG 图像)。
- 免费开源，广泛兼容。

您会找到有创意的用例。

□ https://paranoiaworks.mobi/ptepc/

[image]
[image]

检查一个网站的安全性

[image] 关键词	病毒检测 自助 预防性
[image] 创建时间	2022年8月28日
[image] **Description**	工具

很多网站的保护性不足，因此黑客们经常毫无顾忌地用病毒感染网站，以获取访客的数据。

Website Security Test - 这项服务可以评估网站的安全，核实是否符合标准，进行测试并检查可能的漏洞。

测试需要一点时间。一旦检查完毕，该工具会产生一个安全等级（A+级到F级），并提供一份关于网站上发现的问题的报告。

当您怀疑一个网站时，可以用它来测试。

 https://www.immuniweb.com/websec/

[image]
[image]

检查一个网站的安全性

[image] 关键词	病毒检测 自助 预防性
[image] 创建时间	2022/08/28
[image] **Description**	工具

很多网站的保护性不足，因此黑客们经常毫无顾忌地用病毒感染网站，以获取访客的数据。

Website Security Test - 这项服务可以评估网站的安全，核实是否符合标准，进行测试并检查可能的漏洞。

测试需要一点时间。一旦检查完毕，该工具会产生一个安全等级（A+级到F级），并提供一份关于网站上发现的问题的报告。

当您怀疑一个网站时，可以用它来测试。

□ https://www.immuniweb.com/websec/

[image]
[image]

远程摄像机/对讲机

[image] 关键词	传输安全 安卓 独居 监测 移动设备
[image] 创建时间	2022年9月8日
[image] **Description**	工具

RemoteVideoCam - 一个安卓应用，允许两台安卓设备在同一本地网络上相互传输视频 和/或音频。

启动后，该应用程序将自动找到其他设备，并开始从其摄像头传输视频。

该应用程序可用于监控房子或院子里的东西，以防备和记录恶意的闯入，或者作为一个对讲机，在没有互联网的时候使用。您会能想到有趣的用例。

 https://github.com/izivkov/RemoteVideoCam

 F-droid: https://f-droid.org/packages/org.avmedia.remotevideocam/

[image]
[image]

远程摄像机/对讲机

[image]	关键词	传输安全 安卓 独居 监测 移动设备
[image]	创建时间	2022/09/08
[image]	**Description**	工具

RemoteVideoCam - 一个安卓应用，允许两台安卓设备在同一本地网络上相互传输视频 和/或音频。

启动后，该应用程序将自动找到其他设备，并开始从其摄像头传输视频。

该应用程序可用于监控房子或院子里的东西，以防备和记录恶意的闯入，或者作为一个对讲机，在没有互联网的时候使用。您会能想到有趣的用例。

 https://github.com/izivkov/RemoteVideoCam

 F-droid: https://f-droid.org/packages/org.avmedia.remotevideocam/

[image]
[image]

检查二维码是否安全

[image] 关键词	QR码 自助 预防性
[image] 创建时间	2022年9月19日
[image] **Description**	工具

网站上的病毒很常见，反病毒软件处理这些病毒没有问题。但二维码是另一回事。毕竟URL是被隐藏的，你不知道它们会通向哪里。

RevealQR - 这项服务可以帮助立即显示QR码背后的内容，并检查其是否有恶意。

 https://revealqr.app/

[image]
[image]

检查二维码是否安全

[image] 关键词	QR码 自助 预防性
[image] 创建时间	2022/09/19
[image] **Description**	工具

网站上的病毒很常见，反病毒软件处理这些病毒没有问题。但二维码是另一回事。毕竟URL是被隐藏的，你不知道它们会通向哪里。

RevealQR - 这项服务可以帮助立即显示QR码背后的内容，并检查其是否有恶意。

 https://revealqr.app/

[image]
[image]

免费Matrix 消息应用

[image]	关键词	传输安全 加密 去中心化 移动设备
[image]	创建时间	2022年9月21日
[image]	**Description**	工具

luffyChat - 一个免费的、非商业性的、Matrix 信息应用，适用于Ubuntu Touch、Android和iOS。

▫发送各种信息、图像和文件
▫语音信息
▫分享位置
▫弹出式通知
▫无限数量的私人和公共群组聊天
▫有成千上万参与者的公共频道
▫发现并加入公开群组
▫黑暗模式
▫用户主题
▫将Matrix ID隐藏在简单的QR码后面
▫表情和贴纸
▫与Element、Nheko、NeoChat和所有其他Matrix应用程序兼容
▫端对端加密
还有更多...

 https://gitlab.com/famedly/fluffychat

F-droid: https://f-droid.org/de/packages/chat.fluffy.fluffychat/

网站：https://fluffychat.im/

网页：https://fluffychat.im/web/

[image]
[image]

免费Matrix 消息应用

[image] 关键词	传输安全 加密 去中心化 移动设备
[image] 创建时间	2022/09/21
[image] **Description**	工具

luffyChat - 一个免费的、非商业性的、Matrix 信息应用，适用于 Ubuntu Touch、Android和iOS。

▫发送各种信息、图像和文件
▫语音信息
▫分享位置
▫弹出式通知
▫无限数量的私人和公共群组聊天
▫有成千上万参与者的公共频道
▫发现并加入公开群组
▫黑暗模式
▫用户主题
▫将Matrix ID隐藏在简单的QR码后面
▫表情和贴纸
▫与Element、Nheko、NeoChat和所有其他Matrix应用程序兼容
▫端对端加密
还有更多...

 https://gitlab.com/famedly/fluffychat

F-droid: https://f-droid.org/de/packages/chat.fluffy.fluffychat/

网站：https://fluffychat.im/

网页：https://fluffychat.im/web/

[image]
[image]

隐藏一个应用程序

[image] 关键词	反间谍 移动设备 预防性
[image] 创建时间	2022/09/22
[image] **Description**	工具

可能不希望任何人知道某个程序已被安装在您的计算机上了；或者，您不希望有人卸载某个应用程序；或者，某个应用程序已被删除，但该条目还留在列表中。

Hide From Uninstall List - 这项服务有助于从已安装程序的列表中隐藏一个应用程序。使用非常简单，您所需要做的只是在服务的主菜单中勾选应用程序名称旁边的方框。

另一个很好的功能是，该工具可保护选定的程序不被卸载，并删除已经被删除的应用程序的信息，这样就不会留下任何痕迹。

仅适用于Wins。

 https://www.sordum.org/11081/hide-from-uninstall-list-v1-1/

[image]
[image]

隐藏一个应用程序

[image] 关键词	反间谍 移动设备 预防性
[image] 创建时间	2022年9月22日
[image] **Description**	工具

可能不希望任何人知道某个程序已被安装在您的计算机上了；或者，您不希望有人卸载某个应用程序；或者，某个应用程序已被删除，但该条目还留在列表中。

Hide From Uninstall List - 这项服务有助于从已安装程序的列表中隐藏一个应用程序。使用非常简单，您所需要做的只是在服务的主菜单中勾选应用程序名称旁边的方框。

另一个很好的功能是，该工具可保护选定的程序不被卸载，并删除已经被删除的应用程序的信息，这样就不会留下任何痕迹。

仅适用于Wins。

 https://www.sordum.org/11081/hide-from-uninstall-list-v1-1/

[image]
[image]

类似YubiKey的虚拟USB设备

[image] 关键词	2FA 密码 预防性
[image] 创建时间	2022年9月26日
[image] **Description**	工具

Virtual FIDO 是一个实现 FIDO2/U2F 协议的虚拟USB设备（如YubiKey）以支持2FA和WebAuthN。

▫Virtual FIDO 通过本地TCP创建一个USB/IP服务器来连接虚拟USB设备。

▫这个USB设备然后模拟USB/CTAP协议，为主机提供U2F/FIDO服务。

https://github.com/bulwarkid/virtual-fido

[image]
[image]

类似YubiKey的虚拟USB设备

[image] 关键词	2FA 密码 预防性
[image] 创建时间	2022/09/26
[image] **Description**	工具

Virtual FIDO 是一个实现 FIDO2/U2F 协议的虚拟USB设备（如YubiKey）以支持2FA和WebAuthN。

▫Virtual FIDO 通过本地TCP创建一个USB/IP服务器来连接虚拟USB设备。

▫这个USB设备然后模拟USB/CTAP协议，为主机提供U2F/FIDO服务。

https://github.com/bulwarkid/virtual-fido

[image]
[image]

安卓系统防火墙

[image] 关键词	安卓 防火墙
[image] 创建时间	2022年9月28日
[image] **Description**	工具

如果您需要阻止您的安卓系统上的任何应用程序访问互联网，而您的智能手机上没有内置的方法，有一个应用程序可以帮助您。

NetGuard - 是一个旨在提供有关其他应用程序的数据使用信息的应用程序，如果这种使用是不受欢迎的，则可以阻止这种使用。

该应用程序可以单独允许或拒绝某个应用程序和地址使用您的 Wi-Fi 和/或移动连接。不需要root权限，它可以阻止已安装的应用程序和系统应用程序。

 https://play.google.com/store/apps/details?id=eu.faircode.netguard

[image]
[image]

安卓系统防火墙

[image] 关键词	安卓 防火墙
[image] 创建时间	2022/09/28
[image] **Description**	工具

如果您需要阻止您的安卓系统上的任何应用程序访问互联网，而您的智能手机上没有内置的方法，有一个应用程序可以帮助您。

NetGuard - 是一个旨在提供有关其他应用程序的数据使用信息的应用程序，如果这种使用是不受欢迎的，则可以阻止这种使用。

该应用程序可以单独允许或拒绝某个应用程序和地址使用您的 Wi-Fi 和/或移动连接。不需要root权限，它可以阻止已安装的应用程序和系统应用程序。

 https://play.google.com/store/apps/details?id=eu.faircode.netguard

[image]
[image]

匿名偏执狂的选择

[image] 关键词	代理 免追踪 暗网
[image] 创建时间	2022年9月29日
[image] **Description**	工具

Cryptostorm 是一个为真正的偏执狂提供的VPN服务。

该服务只在Tor和I2P中提供。

1. 不保留日志，并提供多跳。

1. 服务器配置是开源的。
   3.连接前访问令牌散列。
   4.以加密货币支付。

1. 使用匿名的DNS。

1. 内置保护，防止通过WebRTC/DNS泄露你的IP。

1. 内置KillSwitch，断开连接时防止泄露。
   …… 以及更多。

 http://stormwayszuh4juycoy4kwoww5gvcu2c4tdtpkup667pdwe4qenzwayd.onion

[image]
[image]

匿名偏执狂的选择

[image]	关键词	代理 免追踪 暗网
[image]	创建时间	2022/09/29
[image]	**Description**	工具

Cryptostorm 是一个为真正的偏执狂提供的VPN服务。

该服务只在Tor和I2P中提供。

1. 不保留日志，并提供多跳。

1. 服务器配置是开源的。
3.连接前访问令牌散列。
4.以加密货币支付。

1. 使用匿名的DNS。

1. 内置保护，防止通过WebRTC/DNS泄露你的IP。

1. 内置KillSwitch，断开连接时防止泄露。
…… 以及更多。

 http://stormwayszuh4juycoy4kwoww5gvcu2c4tdtpkup667pdwe4qenzwayd.onion

[image]
[image]

在断网后保持通信

[image] 关键词	反封锁 移动设备
[image] 创建时间	2022年10月2日
[image] **Description**	工具

一些可以在断网后保持通信的IM：

Air Chat - 通过蓝牙发送加密的私密消息。为iOS下载。

Divvy - 在没有互联网的情况下也能工作，但范围有限，有一个选项可以创建一个最多7人的聊天。为iOS下载。

Briar - 面向安全的即时通信，更像一个对讲机。在开始沟通之前，你需要先扫描对话者的二维码。仅适用于安卓。

Bridgefy - 允许你向一个区域范围内的所有人发送短信。适用于安卓。

[image]
[image]

在断网后保持通信

[image]	关键词	反封锁 移动设备
[image]	创建时间	2022/10/02
[image]	**Description**	工具

一些可以在断网后保持通信的IM：

Air Chat - 通过蓝牙发送加密的私密消息。为iOS下载。

Divvy - 在没有互联网的情况下也能工作，但范围有限，有一个选项可以创建一个最多7人的聊天。为iOS下载。

Briar - 面向安全的即时通信，更像一个对讲机。在开始沟通之前，你需要先扫描对话者的二维码。仅适用于安卓。

Bridgefy - 允许你向一个区域范围内的所有人发送短信。适用于安卓。

[image]
[image]

一系列安全工具

[image] 关键词	代理 传输安全 免追踪 自助
[image] 创建时间	2022年10月4日
[image] **Description**	工具

I2P In Private Browsing - Mozilla Firefox 浏览器的一个扩展，可以让您安全、方便地使用I2P网络。

hVPN - Hacken Club 的VPN服务。无日志，加密，90天免费试用。

InviZible Pro - 由DNSCrypt、Tor 和 Purple I2P 组成的综合应用。用于实现最大化的安全，隐私并舒适地使用互联网。对于安卓用户。

Amnezia - 是一个免费的应用程序，只需点击几下就可以创建自己的VPN。Windows 和 MacOS 支持。

https://vpnlove.me/ - RosComSvoboda网站，该网站收集了具有高信任度的VPN服务。

WebRTC Leak Shield - 是一个浏览器扩展，可以防止您的IP地址通过WebRTC泄露。

Cover Your Tracks - 是一个服务检查器，它允许您找出浏览器收集了哪些关于您的信息。

Webtor - 下载和播放种子的服务，只需粘贴磁力链接或打开 torrent

文件，然后通过您的网络浏览器安全匿名地开始下载或观看 torrent 内容。无需注册。

Proxy6 - 一个用来检查您的匿名性的和值得信赖的代理商店。

Tinfoil Chat - 另一个为真正的偏执狂提供的安全即时通信工具。开源。

AnonYou - 一个多合一的匿名工具：所有流量经过Tor，改变设备的MAC地址，删除系统日志，交换空间擦除，等等。

Simple DNSCrypt - 一个简单的工具，供Windows用户管理和配置 dnscrypt-proxy。

Algo VPN - 一组ansible脚本，可简化个人 WireGuard 和 IPsecVPN 的设置。

Tallow - 是一个面向Windows用户的透明Tor防火墙和代理解决方案。您的所有互联网流量都将通过Tor网络透明地自动重定向，应用程序不会知道流量已转移。

[image]
[image]

一系列安全工具

[image] 关键词	代理 传输安全 免追踪 自助
[image] 创建时间	2022/10/04
[image] **Description**	工具

I2P In Private Browsing - Mozilla Firefox 浏览器的一个扩展，可以让您安全、方便地使用I2P网络。

hVPN - Hacken Club 的VPN服务。无日志，加密，90天免费试用。

InviZible Pro - 由DNSCrypt、Tor 和 Purple I2P 组成的综合应用。用于实现最大化的安全，隐私并舒适地使用互联网。对于安卓用户。

Amnezia - 是一个免费的应用程序，只需点击几下就可以创建自己的VPN。Windows 和 MacOS 支持。

https://vpnlove.me/ - RosComSvoboda网站，该网站收集了具有高信任度的VPN服务。

WebRTC Leak Shield - 是一个浏览器扩展，可以防止您的IP地址通过WebRTC泄露。

Cover Your Tracks - 是一个服务检查器，它允许您找出浏览器收集了哪些关于您的信息。

Webtor - 下载和播放种子的服务，只需粘贴磁力链接或打开 torrent

文件，然后通过您的网络浏览器安全匿名地开始下载或观看 torrent 内容。无需注册。

Proxy6 - 一个用来检查您的匿名性的和值得信赖的代理商店。

Tinfoil Chat - 另一个为真正的偏执狂提供的安全即时通信工具。开源。

AnonYou - 一个多合一的匿名工具：所有流量经过Tor，改变设备的MAC地址，删除系统日志，交换空间擦除，等等。

Simple DNSCrypt - 一个简单的工具，供Windows用户管理和配置 dnscrypt-proxy。

Algo VPN - 一组ansible脚本，可简化个人 WireGuard 和 IPsecVPN 的设置。

Tallow - 是一个面向Windows用户的透明Tor防火墙和代理解决方案。您的所有互联网流量都将通过Tor网络透明地自动重定向，应用程序不会知道流量已转移。

[image]
[image]

临时/一次性电子邮件服务选项

[image] 关键词	免追踪 电邮
[image] 创建时间	2022/10/09
[image] **Description**	工具

1. https://maildrop.cc/

1. https://erine.email/

1. https://privatlab.com/

1. https://mailsac.com/

1. https://temporarymail.com/

1. https://tempmail.plus

1. https://10minutemail.net/

1. https://emailfake.com/

1. https://www.fakemail.net/

1. https://www.dispostable.com/

1. https://temp-mail.to/

1. http://mailcatch.com

1. https://www.guerrillamail.com/

1. https://www.mailinator.com/

1. https://www.emailondeck.com/

1. https://yopmail.com/en/

1. https://www.33mail.com/

1. https://www.moakt.com/

1. http://mailcatch.com/en/disposable-email

1. http://mytrashmail.com/

1. https://www.emaildrop.io/

1. https://tempr.email/en/

1. https://www.mohmal.com/en

1. https://www.tempinbox.xyz/

[image]
[image]

临时/一次性电子邮件服务选项

[image] 关键词	免追踪 电邮
[image] 关联	[image]一些较安全的电邮客户端选项 ；[image]隐私型电邮提供商的列表
[image] 创建时间	2022年10月9日
[image] **Description**	工具

1. https://maildrop.cc/

1. https://erine.email/

1. https://privatlab.com/

1. https://mailsac.com/

1. https://temporarymail.com/

1. https://tempmail.plus

1. https://10minutemail.net/

1. https://emailfake.com/

1. https://www.fakemail.net/

1. https://www.dispostable.com/

1. https://temp-mail.to/

1. http://mailcatch.com

1. https://www.guerrillamail.com/

1. https://www.mailinator.com/

1. https://www.emailondeck.com/

1. https://yopmail.com/en/

1. https://www.33mail.com/

1. https://www.moakt.com/

1. http://mailcatch.com/en/disposable-email

1. http://mytrashmail.com/

1. https://www.emaildrop.io/

1. https://tempr.email/en/

1. https://www.mohmal.com/en

1. https://www.tempinbox.xyz/

1. https://beeinbox.com/

1. https://temporarymail.app/

1. https://tempmailbox.net/

1. https://tempmail.ing/

1. https://tempmail.rip/

1. https://tempmailg.com/

1. https://mailpoof.com/

1. https://mailgw.com/

1. https://simplelogin.io/

1. https://burnermail.io/

1. https://trashmail.com/

1. https://tememail.org/

1. https://temporaryemail.in/

1. https://tempmailmaster.io/

1. https://tempmail100.com/

1. https://boomlify.com/

1. https://firetempmail.com/

1. https://tmpinbox.com/

1. https://www.tempmail.sbs/

1. https://internxt.com/temporary-email

[image]
[image]

在安卓上隔离老大哥程序

[image] 关键词	反间谍 安卓 沙箱 自助 预防性
[image] 创建时间	2022/10/11
[image] Description	工具

Insular 是一个安卓沙箱环境，用于克隆选定的 "老大哥"应用程序，并隔离它们避免其访问沙箱外的个人数据（包括通话记录、联系人、照片等），即使授予适当的权限。

与设备相关的数据（短信、IMEI等）仍然可用。

一个单独的应用程序可以根据要求被冻结，启动图标消失，其后台行为被完全被阻止。

 https://gitlab.com/secure-system/Insular

F-droid: https://f-droid.org/packages/com.oasisfeng.island.fdroid/

网站：https://secure-system.gitlab.io/Insular/

[image]
[image]

在安卓上隔离老大哥程序

[image]	关键词	反间谍 安卓 沙箱 自助 预防性
[image]	创建时间	2022年10月11日
[image]	**Description**	工具

Insular 是一个安卓沙箱环境，用于克隆选定的 "老大哥"应用程序，并隔离它们避免其访问沙箱外的个人数据（包括通话记录、联系人、照片等），即使授予适当的权限。

与设备相关的数据（短信、IMEI等）仍然可用。

一个单独的应用程序可以根据要求被冻结，启动图标消失，其后台行为被完全阻止。

https://gitlab.com/secure-system/Insular

F-droid: https://f-droid.org/packages/com.oasisfeng.island.fdroid/

网站：https://secure-system.gitlab.io/Insular/

[image]
[image]

开源点对点社交网络

[image] 关键词	反封锁 电脑 社交网络 移动设备 自托管
[image] 关联	[image]去中心化的社交网络协议
[image] 创建时间	2022年10月18日
[image] **Description**	工具

Manyverse - 是一个基于SSB的点对点应用程序/社交网络，可用于电脑和移动设备。

帖子、点赞、个人资料、私人消息等等，所有社交网络的功能它都有。它不会在公司拥有的云中运行，相反，匿名的朋友的帖子和您所有的社交数据都完全存储在您自己的设备上。

因此，即使是离线的时候，您也可以滚动浏览，阅读任何东西，甚至发布和点赞的内容。当您的手机重新连接时，它会通过共享的本地Wi-Fi、蓝牙或互联网将最新的更新直接同步到您的朋友的手机上。

 https://gitlab.com/staltz/manyverse

网站：https://www.manyver.se/

F-droid: https://f-droid.org/packages/se.manyver/

[image]
[image]

开源点对点社交网络

[image]	关键词	反封锁 电脑 社交网络 移动设备 自托管
[image]	创建时间	2022/10/18
[image]	Description	工具

Manyverse - 是一个基于SSB的点对点应用程序/社交网络，可用于电脑和移动设备。

帖子、点赞、个人资料、私人消息等等，所有社交网络的功能它都有。它不会在公司拥有的云中运行，相反，匿名的朋友的帖子和您所有的社交数据都完全存储在您自己的设备上。

因此，即使是离线的时候，您也可以滚动浏览，阅读任何东西，甚至发布和点赞的内容。当您的手机重新连接时，它会通过共享的本地Wi-Fi、蓝牙或互联网将最新的更新直接同步到您的朋友的手机上。

 https://gitlab.com/staltz/manyverse

网站：https://www.manyver.se/

F-droid: https://f-droid.org/packages/se.manyver/

[image]
[image]

Tor上的加密邮件服务

[image] 关键词	传输安全 暗网 电邮
[image] 创建时间	2022年10月21日
[image] **Description**	工具

去与互联网通信的能力。

特点：

- 完全支持PGP加密。
- VMAT协议（可以使用没有 .onion 的普通邮件地址）。
- 默认情况下为SSL加密（STARTTLS 2048 位）。
- 隐藏了所有种类的元数据。
- 所有连接只通过Tor进行。
- 强大的加密技术。
- 无限数量的邮件别名。
- 兼容SMTP。

…………还有更多。

 https://en.onionmail.info/what.html

[image]
[image]

Tor上的加密邮件服务

[image]	关键词	传输安全 暗网 电邮
[image]	创建时间	2022/10/21
[image]	**Description**	工具

去与互联网通信的能力。

特点：

- 完全支持PGP加密。
- VMAT协议（可以使用没有 .onion 的普通邮件地址）。
- 默认情况下为SSL加密（STARTTLS 2048 位）。
- 隐藏了所有种类的元数据。
- 所有连接只通过Tor进行。
- 强大的加密技术。
- 无限数量的邮件别名。
- 兼容SMTP。

…………还有更多。

https://en.onionmail.info/what.html

[image]
[image]

也是隐写

[image] 关键词	传输安全 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2022年10月23日
[image] Description	工具

OpenStego - 是一个隐写术应用程序，提供两种功能。

▫ 隐藏数据：它可以将任何数据隐藏在图像文件中。
▫ 水印：用不可见的签名给图像文件加水印，可用于检测未经授权的文件复制。

在 GNU/Linux/MacOS/Windows 中工作。

 https://github.com/syvaidya/openstego

网站：https://www.openstego.com/

[image]
[image]

也是隐写

[image]	关键词	传输安全 隐写术
[image]	创建时间	2022/10/23
[image]	**Description**	工具

OpenStego - 是一个隐写术应用程序，提供两种功能。

▫ 隐藏数据：它可以将任何数据隐藏在图像文件中。
▫ 水印：用不可见的签名给图像文件加水印，可用于检测未经授权的文件复制。

在 GNU/Linux/MacOS/Windows 中工作。

 https://github.com/syvaidya/openstego

网站：https://www.openstego.com/

[image]
[image]

恢复误删除的数据

[image] 关键词	数据丢失 自助
[image] 创建时间	2022/10/29
[image] **Description**	工具

TestDisk是一个强大的、免费的程序，可以恢复在各种情况下删除的数据：由于恶意软件、错误、系统故障、或整个磁盘分区的意外删除。

它能做什么：

- 修复分区表，恢复被删除的分区
- 从备份中恢复 FAT32 引导扇区
- 重建 FAT12/FAT16/FAT32 引导扇区
- 修复 FAT 表
- 重建 NTFS 引导扇区
- 从备份中恢复 NTFS 引导扇区
- 使用 MFT 镜像修复 MFT

- 从已删除的 FAT、NTFS 和 ext2/ext3/ext4 分区复制文件。

TestDisk 适合新手使用。

 https://www.cgsecurity.org/wiki/TestDisk_CN

还有另一个具有类似功能和更直观界面的软件 Recuva：

 https://www.ccleaner.com/recuva

[image]
[image]

恢复误删除的数据

[image]	关键词	数据丢失 自助
[image]	创建时间	2022年10月29日
[image]	**Description**	工具

TestDisk是一个强大的、免费的程序，可以恢复在各种情况下删除的数据：由于恶意软件、错误、系统故障、或整个磁盘分区的意外删除。

它能做什么：

- 修复分区表，恢复被删除的分区
- 从备份中恢复 FAT32 引导扇区
- 重建 FAT12/FAT16/FAT32 引导扇区
- 修复 FAT 表
- 重建 NTFS 引导扇区
- 从备份中恢复 NTFS 引导扇区
- 使用 MFT 镜像修复 MFT

- 从已删除的 FAT、NTFS 和 ext2/ext3/ext4 分区复制文件。

TestDisk 适合新手使用。

 https://www.cgsecurity.org/wiki/TestDisk_CN

还有另一个具有类似功能和更直观界面的软件 Recuva：

 https://www.ccleaner.com/recuva

[image]
[image]

插拔传输代理工具

[image] 关键词	代理 免追踪
[image] 创建时间	2022/10/30
[image] **Description**	工具

Cloak 是一个可插拔传输工具，它扩展了传统代理工具的功能，如Shadowsocks、OpenVPN和Tor，以避免复杂的审查和数据歧视。

Cloak不是一个独立的代理程序。相反，它的工作原理是将代理流量伪装成普通网络浏览。

传统工具的流量指纹太明显，而Cloak则很难准确被识别。这增加了审查行动的附带损害，因为试图阻止Cloak的行动也会损害审查国家所依赖的服务。

 https://github.com/cbeuw/Cloak

[image]
[image]

插拔传输代理工具

[image]	关键词	代理 免追踪
[image]	创建时间	2022年10月30日
[image]	**Description**	工具

Cloak 是一个可插拔传输工具，它扩展了传统代理工具的功能，如Shadowsocks、OpenVPN和Tor，以避免复杂的审查和数据歧视。

Cloak不是一个独立的代理程序。相反，它的工作原理是将代理流量伪装成普通网络浏览。

传统工具的流量指纹太明显，而Cloak则很难准确被识别。这增加了审查行动的附带损害，因为试图阻止Cloak的行动也会损害审查国家所依赖的服务。

https://github.com/cbeuw/Cloak

[image]
[image]

安全笔记管理

[image]	关键词	加密 反侦察
[image]	创建时间	2022/10/31
[image]	**Description**	工具

Safe-Notes 是一个注重隐私的笔记管理器，提供内置的加密存储。

▫AES-256加密存储
▫可以以加密和未加密的形式导出数据
▫加密或未加密的导入选项
▫黑暗/光明主题
▫可顺利迁移到新设备上
▫完全匿名，没有入站或出站请求

https://github.com/keshav-space/safenotes

F-droid: https://f-droid.org/packages/com.trisven.safenotes/

[image]
[image]

安全笔记管理

[image] 关键词		加密 反侦察
[image] 创建时间		2022年10月31日
[image] **Description**		工具

Safe-Notes 是一个注重隐私的笔记管理器，提供内置的加密存储。

▫AES-256加密存储
▫可以以加密和未加密的形式导出数据
▫加密或未加密的导入选项
▫黑暗/光明主题
▫可顺利迁移到新设备上
▫完全匿名，没有入站或出站请求

https://github.com/keshav-space/safenotes

F-droid: https://f-droid.org/packages/com.trisven.safenotes/

[image]
[image]

加密文件管理

[image] 关键词	加密 查询整理
[image] 创建时间	2022年11月2日
[image] **Description**	工具

PeaZip - 是一个简单的、免费的文件存档和解密工具，适用于Windows、BSD和GNU/Linux。

它能处理200多种存档格式（7z, ace, arc, bz2, cab, gz, iso, paq, pea, rar, tar, wim, zip, zipx ...），能处理跨区存档（001, r01, z01）并支持多种存档加密标准，文件散列。

同时支持GUI和CLI。

 https://github.com/peazip/PeaZip

网站：https://peazip.github.io/

[image]
[image]

加密文件管理

[image] 关键词	加密 查询整理
[image] 创建时间	2022/11/02
[image] **Description**	工具

PeaZip - 是一个简单的、免费的文件存档和解密工具，适用于Windows、BSD和GNU/Linux。

它能处理200多种存档格式（7z, ace, arc, bz2, cab, gz, iso, paq, pea, rar, tar, wim, zip, zipx ...），能处理跨区存档（001, r01, z01）并支持多种存档加密标准，文件散列。

同时支持GUI和CLI。

 https://github.com/peazip/PeaZip

网站：https://peazip.github.io/

[image]
[image]

检查您的代理是否真的起到保护作用

[image] 关键词		代理 自检
[image] 创建时间		2022年11月3日
[image] **Description**		工具

Do I Leak? - 是一个全面的检查器，您可以在采取保护措施之后用它进行检查。

- 通过WebRTC检查您在VPN下是否IP泄漏。
- 通过您的洪流客户端检查是否有IP地址泄漏。
- 检查是否有DNS泄漏。
- 检查HTML5地理位置的泄漏。

 https://www.top10vpn.com/tools/do-i-leak/

[image]
[image]

检查您的代理是否真的起到保护作用

[image] 关键词	代理 自检
[image] 创建时间	2022/11/03
[image] **Description**	工具

Do I Leak? - 是一个全面的检查器，您可以在采取保护措施之后用它进行检查。

- 通过WebRTC检查您在VPN下是否IP泄漏。
- 通过您的洪流客户端检查是否有IP地址泄漏。
- 检查是否有DNS泄漏。
- 检查HTML5地理位置的泄漏。

 https://www.top10vpn.com/tools/do-i-leak/

[image]
[image]

一些匿名的电邮选择

[image] 关键词	免追踪 电邮
[image] 创建时间	2022年11月15日
[image] **Description**	工具

1. Simple Login 是一项匿名的电子邮件中转服务，以保护您免受垃圾邮件和数据收集的影响。不仅可以接收电子邮件，还可以匿名回复。可与Thunderburd和Mailpile良好整合。

1. AnonAddy 是一个匿名的开源电子邮件服务，用于反垃圾邮件保护。能够识别哪个网站出售了您的电子邮件地址。您可以用其匿名回复邮件。

1. Onion Mail 是一个匿名和加密的邮件服务器，可在Tor网络和其他地方工作。邮件别名的数量不限。隐藏各种元数据，所有连接仅通过 Tor，强加密，以及更多功能。

1. Firefox Relay - 是一个官方的Firefox插件，允许您创建电子邮件别名，可以用来转发电子邮件到您的真实邮箱。

1. SpamGourmet - 可自毁的电子邮件地址，功能非常广泛，为每封发送的电子邮件生成一个临时电子邮件地址。

[image]
[image]

一些匿名的电邮选择

[image] 关键词	免追踪 电邮
[image] 创建时间	2022/11/15
[image] **Description**	工具

1. Simple Login 是一项匿名的电子邮件中转服务，以保护您免受垃圾邮件和数据收集的影响。不仅可以接收电子邮件，还可以匿名回复。可与Thunderburd和Mailpile良好整合。

1. AnonAddy 是一个匿名的开源电子邮件服务，用于反垃圾邮件保护。能够识别哪个网站出售了您的电子邮件地址。您可以用其匿名回复邮件。

1. Onion Mail 是一个匿名和加密的邮件服务器，可在Tor网络和其他地方工作。邮件别名的数量不限。隐藏各种元数据，所有连接仅通过 Tor，强加密，以及更多功能。

1. Firefox Relay - 是一个官方的Firefox插件，允许您创建电子邮件别名，可以用来转发电子邮件到您的真实邮箱。

1. SpamGourmet - 可自毁的电子邮件地址，功能非常广泛，为每封发送的电子邮件生成一个临时电子邮件地址。

[image]
[image]

调查区块链上的交易

[image] 关键词	加密货币 自检 预防性
[image] 关联	[image]免 KYC 的交易平台（精选）；[image]绕开KYC 的情况下用加密货币交换加密货币的方法；调查区块链上的交易；隐私堡垒门罗币 - 服务清单**2026**：钱包、交易所、匿名**SIM**卡、主机及其他
[image] 创建时间	2022年11月17日
[image] **Description**	工具

关于如何调查区块链上的交易呢，这里有一个工具列表:

· explorer.bitquery.io
• phalcon.blocksec.com
• explorer.0x.org
• socketscan.io
• cruise.supremacy.team
• blockscout.com
• ethplorer.io
• amlbot.com
• tenderly.co
• ethtective.com
• breadcrumbs.app
• 9000.hal.xyz
• bloxy.info
• oko.palkeo.com
• zeromev.org
• dune.xyz

- github.com/naddison36/tx2uml
- github.com/ApeWorX/evm-trace
- nansen.ai
- oxt.me
- misttrack.io
- blockpath.com
- graphsense.info
- tutela.xyz
- impersonator.xyz
- maltego.com/transform-hub/tatum-blockchain-explorer/
- github.com/Cryptonomic/Arronax
- github.com/s0md3v/Orbit

ETH-USDT flow:

dune.com/runstar/eth-usdt-flow?address_t360d6=0x0f1ccd7DB92209B5FAE43Cfe5c98B66d1757Aa79&汇总USDT最小转移量_nbcc80=0&单笔USDT最小转移量_n8de76=0

[image]
[image]

调查区块链上的交易

[image]	关键词	加密货币 自检 预防性
[image]	创建时间	2022/11/17
[image]	**Description**	工具

关于如何调查区块链上的交易呢，这里有一个工具列表:

- explorer.bitquery.io
- phalcon.blocksec.com
- explorer.0x.org
- socketscan.io
- cruise.supremacy.team
- blockscout.com
- ethplorer.io
- amlbot.com
- tenderly.co
- ethtective.com
- breadcrumbs.app
- 9000.hal.xyz
- bloxy.info
- oko.palkeo.com
- zeromev.org
- dune.xyz
- github.com/naddison36/tx2uml
- github.com/ApeWorX/evm-trace
- nansen.ai
- oxt.me
- misttrack.io
- blockpath.com
- graphsense.info

- tutela.xyz
- impersonator.xyz
- maltego.com/transform-hub/tatum-blockchain-explorer/
- github.com/Cryptonomic/Arronax
- github.com/s0md3v/Orbit

ETH-USDT flow:

dune.com/runstar/eth-usdt-flow?address_t360d6=0x0f1ccd7DB92209B5FAE43Cfe5c98B66d1757Aa79&汇总USDT最小转移量_nbcc80=0&单笔USDT最小转移量_n8de76=0

[image]
[image]

安全的云中存储

[image]	关键词	云存储 元数据 加密 查询整理 自托管
[image]	创建时间	2022/11/18
[image]	**Description**	工具

1. Cryptee - 是一项限量免费的服务，用于安全地存储文档、文件和照片。完全开源。注册是匿名的。

1. e2ee云 - 具有端到端加密功能的开源云存储，自托管。

1. Filen — zero-knowledge - 是一个e2e云，有10GB空间的免费计划。

1. Nextcloud - 是一套免费和开源的客户端-服务器程序，用于在私人服务器上创建自己的文件共享。是DropBox、Google Drive或Office 365的替代品。在这里看到更多：https://iyouport.substack.com/p/nextcloud-

1. MEGA - 是一项古老的服务，不需要介绍了。使用端到端加密，20GB免费。

1. Peergos - 安全的p2p文件存储+社交网络，抗量子破解的端对端加密，受保护的元数据。Peergos本质上是一个去中心化的网络，具有上传、存储和分享文件的能力。

1. Tahoe-LAFS - 是一项免费开源的分散式云存储服务。

[image]
[image]

安全的云中存储

[image]	关键词	云存储 元数据 加密 查询整理 自托管
[image]	创建时间	2022年11月18日
[image]	**Description**	工具

1. Cryptee - 是一项限量免费的服务，用于安全地存储文档、文件和照片。完全开源。注册是匿名的。

1. e2ee云 - 具有端到端加密功能的开源云存储，自托管。

1. Filen — zero-knowledge - 是一个e2e云，有10GB空间的免费计划。

1. Nextcloud - 是一套免费和开源的客户端-服务器程序，用于在私人服务器上创建自己的文件共享。是DropBox、Google Drive或Office 365的替代品。在这里看到更多：https://iyouport.substack.com/p/nextcloud-

1. MEGA - 是一项古老的服务，不需要介绍了。使用端到端加密，20GB免费。

1. Peergos - 安全的p2p文件存储+社交网络，抗量子破解的端对端加密，受保护的元数据。Peergos本质上是一个去中心化的网络，具有上传、存储和分享文件的能力。

1. Tahoe-LAFS - 是一项免费开源的分散式云存储服务。

[image]
[image]

将任何网站变成PDF文件

[image] 关键词	反封锁 查询整理
[image] 创建时间	2022/11/19
[image] **Description**	工具

在某些情况下，您可能有需要在没有互联网的情况下打开一个信息网站。这方面的最佳解决方案是使用 Printfriendly 服务将网站变成一个PDF文件。

做法很简单：

1.打开主页，插入一个所需网站的链接，然后点击 "预览"。
2. 如果有必要，您也可以在这里编辑一下。
3. 产生的文件可以下载、通过电子邮件发送、或立即打印出纸质文件。

 https://www.printfriendly.com/

[image]
[image]

将任何网站变成PDF文件

[image] 关键词	反封锁 查询整理
[image] 创建时间	2022年11月19日
[image] **Description**	工具

在某些情况下，您可能有需要在没有互联网的情况下打开一个信息网站。这方面的最佳解决方案是使用 Printfriendly 服务将网站变成一个PDF文件。

做法很简单：

1.打开主页，插入一个所需网站的链接，然后点击 "预览"。
2. 如果有必要，您也可以在这里编辑一下。
3. 产生的文件可以下载、通过电子邮件发送、或立即打印出纸质文件。

 https://www.printfriendly.com/

[image]
[image]

开源电邮客户端

[image]	关键词	传输安全 加密 电邮
[image]	创建时间	2022年11月22日
[image]	**Description**	工具

Roundcube是一个安全、开源的电子邮件客户端。

- 用户友好的桌面版。
- 可定制的用户界面。
- PGP加密。
- 多语种。
- 多个发件人身份。
- 导入/导出功能。
- XSS攻击防护。
  以及更多 ……

 https://roundcube.net/

[image]
[image]

开源电邮客户端

[image]	关键词	传输安全 加密 电邮
[image]	创建时间	2022/11/22
[image]	**Description**	工具

Roundcube是一个安全、开源的电子邮件客户端。

- 用户友好的桌面版。
- 可定制的用户界面。
- PGP加密。
- 多语种。
- 多个发件人身份。
- 导入/导出功能。
- XSS攻击防护。
  以及更多 ……

 https://roundcube.net/

[image]
[image]

一系列安全的即时通信软件和服务

[image]	关键词	IMs P2P tor 传输安全 免追踪 去中心化
[image]	创建时间	2022/11/23
[image]	**Description**	工具

1. E2EE + 开源

Session

Delta Chat

Simplex Chat

Wire

2. Matrix客户端

Element

Syphon

Cinny

FluffyChat

SchildiChat

3. 离线可用(网状网络)

berty

dIM Chat

Rumble

Serval Mesh

FireChat

Meshenger

Berkanan

Mesh

4. 基于Tor

Tinfoil Chat

Ricochet Refresh

Briar

Tox

Speek

cwtch.im

5. 区块链

Status

Mixin

Adamant

iMe Messenger & Crypto Wallet

6. 分叉

Molly (Signal)

DarkMessenger (Conversations)

aTox 0.6.0 (Tox)

Taranis (Jami)

7. VOIP/SIP/视频通话

Jami

Pryvate Now

Rocket.Chat

Jitsi Meet

Sipnetic

Linphone

VIPole

8. XMPP (OTR/OMEMO)

Conversations

CoyIM

Dino.

Pidgin

Gajim

blabber

Beagle

MirandaNG

Wime

ChatSecure

[image]
[image]

一系列安全的即时通信软件和服务

[image]	关键词	IMs P2P tor 传输安全 免追踪 去中心化
[image]	创建时间	2022年11月23日
[image]	**Description**	工具

1. E2EE ＋ 开源

Session

Delta Chat

Simplex Chat

Wire

2. Matrix客户端

Element

Syphon

Cinny

FluffyChat

SchildiChat

3. 离线可用(网状网络)

berty

dIM Chat

Rumble

Serval Mesh

FireChat

Meshenger

Berkanan

Mesh

4. 基于Tor

Tinfoil Chat

Ricochet Refresh

Briar

Tox

Speek

cwtch.im

5. 区块链

Status

Mixin

Adamant

iMe Messenger & Crypto Wallet

6. 分叉

Molly (Signal)

DarkMessenger (Conversations)

aTox 0.6.0 (Tox)

Taranis (Jami)

7. VOIP/SIP/视频通话

Jami

Pryvate Now

Rocket.Chat

Jitsi Meet

Sipnetic

Linphone

VIPole

8. XMPP (OTR/OMEMO)

Conversations

CoyIM

Dino.

Pidgin

Gajim

blabber

Beagle

MirandaNG

Wime

ChatSecure

[image]
[image]

一些较安全的电邮客户端选项

[image] 关键词	加密 电邮
[image] 关联	[image]隐私型电邮提供商的列表
[image] 创建时间	2022年11月25日
[image] **Description**	工具

1. Cypht - 模块化的电子邮件客户端，有很多插件，轻量级，RSS新闻源：https://cypht.org/index.html

1. Squirrelmail - 老旧但可靠的轻量级电子邮件客户端，设计简约，支持PGP加密：https://www.squirrelmail.org/

1. Rainloop - 没有数据存储在服务器上，默认OpenPGP加密：https://www.rainloop.net/

1. Horde - 极简的，类似于Squirrelmail的PHP邮件客户端：https://www.horde.org/

1. Afterlogic WebMail Lite - 支持整合各种服务的客户端，OpenPGP加密：https://afterlogic.org/webmail-lite

1. PREVEIL - 免费的电子邮件客户端，具有端到端加密和安全云存储功能：https://www.preveil.com/

1. TorBirdy - Mozilla Thunderbird 邮件客户端的扩展，它允许您

通过Tor网络连接和发送电子邮件：https://addons.thunderbird.net/en-GB/thunderbird/addon/torbirdy/

1. Claws Mail - 是一个基于GTK+的免费开源邮件客户端（和新闻阅读器）。易于配置，功能丰富：https://www.claws-mail.org/

1. K-9 Mail - 是一个为安卓用户提供的开源电子邮件客户端。可以说是相比下最好的一个：https://k9mail.app/

[image]
[image]

一些较安全的电邮客户端选项

[image] 关键词	加密 电邮
[image] 创建时间	2022/11/25
[image] **Description**	工具

1. Cypht - 模块化的电子邮件客户端，有很多插件，轻量级，RSS新闻源：https://cypht.org/index.html

1. Squirrelmail - 老旧但可靠的轻量级电子邮件客户端，设计简约，支持PGP加密：https://www.squirrelmail.org/

1. Rainloop - 没有数据存储在服务器上，默认OpenPGP加密：https://www.rainloop.net/

1. Horde - 极简的，类似于Squirrelmail的PHP邮件客户端：https://www.horde.org/

1. Afterlogic WebMail Lite - 支持整合各种服务的客户端，OpenPGP加密：https://afterlogic.org/webmail-lite

1. PREVEIL - 免费的电子邮件客户端，具有端到端加密和安全云存储功能：https://www.preveil.com/

1. TorBirdy - Mozilla Thunderbird 邮件客户端的扩展，它允许您通过Tor网络连接和发送电子邮件：https://addons.thunderbird.net/en-GB/thunderbird/addon/torbirdy/

1. Claws Mail - 是一个基于GTK+的免费开源邮件客户端（和新闻阅读器）。易于配置，功能丰富：https://www.claws-mail.org/

1. K-9 Mail - 是一个为安卓用户提供的开源电子邮件客户端。可以说是相比下最好的一个：https://k9mail.app/

[image]
[image]

可自托管的匿名pastebin

[image]	关键词	传输安全 加密 自托管 阅后即焚
[image]	创建时间	2022/11/26
[image]	**Description**	工具

Pasteburn - 另一个可自托管的匿名pastebin，开源，可阅后即焚。端对端加密。

您可以决定在一定数量的独立访客获取内容之后、或一定时间过后，让内容消失。

将一些内容粘贴到 Pasteburn 中后，将 URL 分享到一般的平台。基于关键词过滤的审查系统或一般的机器人将无法解密或识别内容。

该信息在您的浏览器中被加密，明文永远不会离开您的浏览器，密码在您本地。

 https://github.com/pasteburn/pasteburn

在线演示可在 pasteburn.onrender.com 中获得。

[image]
[image]

可自托管的匿名pastebin

[image] 关键词	传输安全 加密 自托管 阅后即焚
[image] 创建时间	2022年11月26日
[image] **Description**	工具

Pasteburn - 另一个可自托管的匿名pastebin，开源，可阅后即焚。端对端加密。

您可以决定在一定数量的独立访客获取内容之后、或一定时间过后，让内容消失。

将一些内容粘贴到 Pasteburn 中后，将 URL 分享到一般的平台。基于关键词过滤的审查系统或一般的机器人将无法解密或识别内容。

该信息在您的浏览器中被加密，明文永远不会离开您的浏览器，密码在您本地。

 https://github.com/pasteburn/pasteburn

在线演示可在 pasteburn.onrender.com 中获得。

[image]
[image]

私密电话号码

[image]	关键词	SMS 手机号 自主 身份验证
[image]	创建时间	2022年12月2日
[image]	**Description**	工具

Private Phone - 私密的虚拟电话号码，用来接收短信的机器人；

- 可以长期租用；
- 使用加密货币（BTC、LTC、USDT、TON 等）支付；
- 有支持呼叫的号码；
- 首次购买可享受 10% 折扣；

Telegram：@PrivatePhoneBot
 https://sms-activate.app/

[image]
[image]

一些可以欺骗智能手机上的地理位置数据的工具

[image] 关键词	免追踪 对抗性思考方式 移动设备
[image] 创建时间	2023年1月30日
[image] **Description**	工具

一些可以欺骗智能手机上的地理位置数据的工具：

iOS

1. Tenorshare iAnyGo：https://www.tenorshare.com/products/ianygo-change-gps-location-iphone.html

1. iSpoofer：https://kubadownload.com/news/ispoofer-ios-ipa/

1. iTools：https://www.itools4.com/

Android

1. Fake GPS Location Go：https://play.google.com/store/apps/details?id=com.xdoapp.virtualphonenavigation

1. FlyGPS：https://play.google.com/store/apps/details?id=com.fly.gps&hl=en&gl=US

1. Fake GPS Location Spoofer：https://play.google.com/store/apps/details?id=com.incorporateapps.fakegps.fre

1. Fake GPS：https://play.google.com/store/apps/details?id=com.blogspot.newapphorizons.fakegps

[image]
[image]

一些可以欺骗智能手机上的地理位置数据的工具

[image] 关键词	免追踪 对抗性思考方式 移动设备
[image] 创建时间	2023/01/30
[image] **Description**	工具

一些可以欺骗智能手机上的地理位置数据的工具：

iOS

1. Tenorshare iAnyGo：https://www.tenorshare.com/products/ianygo-change-gps-location-iphone.html

1. iSpoofer：https://kubadownload.com/news/ispoofer-ios-ipa/

1. iTools：https://www.itools4.com/

Android

1. Fake GPS Location Go：https://play.google.com/store/apps/details?id=com.xdoapp.virtualphonenavigation

1. FlyGPS：https://play.google.com/store/apps/details?id=com.fly.gps&hl=en&gl=US

1. Fake GPS Location Spoofer：https://play.google.com/store/apps/details?id=com.incorporateapps.fakegps.fre

1. Fake GPS：https://play.google.com/store/apps/details?id=com.blogspot.newapphorizons.fakegps

[image]
[image]

在Android上加密文件

[image]	关键词	加密 安卓 密码
[image]	创建时间	2023年2月1日
[image]	**Description**	工具

SSE是一个用于加密所有类型的文件、文档、视频和照片的应用程序。对文件夹、目录和笔记进行加密。含隐写。它使用以下加密算法：

- AES（Rijndael）256
- RC6 256
- Serpent 256
- Blowfish 448
- Twofish 256 等。

附加功能：密码管理器和密码生成器。

 https://play.google.com/store/apps/details?id=com.paranoiaworks.unicus.android.sse&hl=en&gl=US&pli=1

[image]
[image]

在Android上加密文件

[image] 关键词	加密 安卓 密码
[image] 创建时间	2023/02/01
[image] **Description**	工具

SSE是一个用于加密所有类型的文件、文档、视频和照片的应用程序。对文件夹、目录和笔记进行加密。含隐写。它使用以下加密算法：

- AES（Rijndael）256
- RC6 256
- Serpent 256
- Blowfish 448
- Twofish 256 等。

附加功能：密码管理器和密码生成器。

 https://play.google.com/store/apps/details?id=com.paranoiaworks.unicus.android.sse&hl=en&gl=US&pli=1

[image]
[image]

专注于隐私的安卓网络浏览器

[image] 关键词	免追踪 安卓 移动设备
[image] 创建时间	2023年2月8日
[image] **Description**	工具

monocles browser - 一个专注于隐私的安卓网络浏览器。

▫ 默认情况下，Javascript和cookies被禁用，以使其尽可能的安全。
▫ 支持Tor Orbot。
▫ 集成了 EasyList 的广告屏蔽功能。
▫ 确保SSL证书的安全。
▫ 导入/导出设置和书签。
▫ https://monocles.de/ 元搜索引擎是默认设置的（声称不保存您的IP和查询）。

https://codeberg.org/Arne/monocles_browser

网站：https://monocles.de/more/

F-droid: https://f-droid.org/packages/de.monocles.browser/

[image]
[image]

专注于隐私的安卓网络浏览器

[image] 关键词	免追踪 安卓 移动设备
[image] 创建时间	2023/02/08
[image] **Description**	工具

monocles browser - 一个专注于隐私的安卓网络浏览器。

▫ 默认情况下，Javascript和cookies被禁用，以使其尽可能的安全。
▫ 支持Tor Orbot。
▫ 集成了 EasyList 的广告屏蔽功能。
▫ 确保SSL证书的安全。
▫ 导入/导出设置和书签。
▫ https://monocles.de/ 元搜索引擎是默认设置的（声称不保存您的IP和查询）。

https://codeberg.org/Arne/monocles_browser

网站：https://monocles.de/more/

F-droid: https://f-droid.org/packages/de.monocles.browser/

[image]
[image]

创建一个加密的相册

[image]	关键词	加密 移动设备
[image]	创建时间	2023年2月9日
[image]	**Description**	工具

1. ente - 一个简单的、端到端加密的、开源的照片存储服务，注重隐私：https://ente.io/

1. stingle Photos - 替代您的智能手机上的常规相册，有加密和备份功能：https://stingle.org/

1. Vault - 一个为安卓用户提供的免费应用程序，允许您创建一个加密的相册，用密码保护它（还可以创建假私密空间来隐藏真实的私密空间）：https://play.google.com/store/apps/details?id=com.netqin.ps

1. Cryptocam - 用于创建加密的照片和视频的应用程序。即使攻击者获得了对您的设备或 SD 卡的物理访问权限，您的数据也是安全的：https://f-droid.org/en/packages/com.tnibler.cryptocam/

1. Calc Box - 假的计算器，在这里您可以隐藏照片和视频：https://play.google.com/store/apps/details?id=calc.gallery.lock

和我们此前介绍过的 Calculator Vault 是类似的。

[image]
[image]

创建一个加密的相册

[image]	关键词	加密 移动设备
[image]	创建时间	2023/02/09
[image]	**Description**	工具

1. ente - 一个简单的、端到端加密的、开源的照片存储服务，注重隐私：https://ente.io/

1. stingle Photos - 替代您的智能手机上的常规相册，有加密和备份功能：https://stingle.org/

1. Vault - 一个为安卓用户提供的免费应用程序，允许您创建一个加密的相册，用密码保护它（还可以创建假私密空间来隐藏真实的私密空间）：https://play.google.com/store/apps/details?id=com.netqin.ps

1. Cryptocam - 用于创建加密的照片和视频的应用程序。即使攻击者获得了对您的设备或 SD 卡的物理访问权限，您的数据也是安全的：https://f-droid.org/en/packages/com.tnibler.cryptocam/

1. Calc Box - 假的计算器，在这里您可以隐藏照片和视频：https://play.google.com/store/apps/details?id=calc.gallery.lock

和我们此前介绍过的 Calculator Vault 是类似的。

[image]
[image]

P2P信使

[image] 关键词	IMs P2P 加密
[image] 创建时间	2023/02/27
[image] **Description**	工具

Mimir是一个真正的p2p信使，在Yggdrasil网络上运行。

- 默认对信息进行端到端加密。
- 全面的权力下放。
- 基于椭圆曲线的认证。
- 直接在设备上工作，所有联系人都可以相互连接，而无需使用中间服务器。Yggdrasil 提供 P2P 连接，不受常规互联网限制。

 https://github.com/Revertron/Mimir

[image]
[image]

P2P信使

[image] 关键词	IMs P2P 加密
[image] 创建时间	2023年2月27日
[image] **Description**	工具

Mimir是一个真正的p2p信使，在Yggdrasil网络上运行。

- 默认对信息进行端到端加密。
- 全面的权力下放。
- 基于椭圆曲线的认证。
- 直接在设备上工作，所有联系人都可以相互连接，而无需使用中间服务器。Yggdrasil 提供 P2P 连接，不受常规互联网限制。

 https://github.com/Revertron/Mimir

[image]
[image]

在手机上隐藏私密文件和应用

[image] 关键词	反侦察 安卓 预防性
[image] 创建时间	2023年3月3日
[image] **Description**	工具

Amarok是一款安卓应用，只需点击一下就可以隐藏个人文件和应用。

 https://github.com/deltazefiro/Amarok-Hider

网站：https://deltazefiro.github.io/Amarok-doc/

F-droid: https://f-droid.org/packages/deltazero.amarok.foss/

[image]
[image]

在手机上隐藏私密文件和应用

[image]	关键词	反侦察 安卓 预防性
[image]	创建时间	2023/03/03
[image]	**Description**	工具

Amarok是一款安卓应用，只需点击一下就可以隐藏个人文件和应用。

 https://github.com/deltazefiro/Amarok-Hider

网站：https://deltazefiro.github.io/Amarok-doc/

F-droid: https://f-droid.org/packages/deltazero.amarok.foss/

[image]
[image]

GPS工具

[image]	关键词	定位
[image]	创建时间	2023年3月6日
[image]	**Description**	工具

推荐一些PGP工具：

1. SeaHorse (Linux/GNOME)：https://wiki.gnome.org/Apps/Seahorse/

1. Kleopatra (Linux/KDE)：https://apps.kde.org/kleopatra/

1. GPG4Win (Windows)：https://www.gpg4win.org/

1. GPG Suite (MacOS)：https://gpgtools.org/

1. OpenKeyChain (Android)：https://www.openkeychain.org/

1. PGP Everywhere (iOS)：https://www.pgpeverywhere.com/

1. FlowCrypt (浏览器)：https://flowcrypt.com/

1. EnigMail (ThunderBird)：https://enigmail.net/index.php/en/

1. GPG4USB (Portable)：https://gpg4usb.org/

[image]
[image]

GPS工具

[image] 关键词	定位
[image] 创建时间	2023/03/06
[image] **Description**	工具

推荐一些PGP工具：

1. SeaHorse (Linux/GNOME)：https://wiki.gnome.org/Apps/Seahorse/

1. Kleopatra (Linux/KDE)：https://apps.kde.org/kleopatra/

1. GPG4Win (Windows)：https://www.gpg4win.org/

1. GPG Suite (MacOS)：https://gpgtools.org/

1. OpenKeyChain (Android)：https://www.openkeychain.org/

1. PGP Everywhere (iOS)：https://www.pgpeverywhere.com/

1. FlowCrypt (浏览器)：https://flowcrypt.com/

1. EnigMail (ThunderBird)：https://enigmail.net/index.php/en/

1. GPG4USB (Portable)：https://gpg4usb.org/

[image]
[image]

VirusTotal的官方浏览器扩展

[image] 关键词	病毒检测 自检
[image] 创建时间	2023年3月12日
[image] **Description**	工具

VirusTotal是一个检查文件是否有病毒和恶意代码的服务，它发布了一个浏览器扩展，即VT4Browsers。

VT4Browsers 允许您发送一个下载的文件到该服务，并检查它是否有病毒。它是在浏览器中下载文件后自动完成的。通过点击扩展名图标，您可以获得有关该文件的信息。

有一些设置。例如，您可以在文件被VirusTotal扫描之前阻止它的打开。可以添加格式例外，如docx或pdf文件将不被发送扫描。该扩展可用于谷歌浏览器和火狐浏览器。

 https://chrome.google.com/webstore/detail/vt4browsers/efbjojhplkelaegfbieplglfidafgoka/related
 https://addons.mozilla.org/en-US/firefox/addon/vt4browsers/

[image]
[image]

VirusTotal的官方浏览器扩展

[image] 关键词	病毒检测 自检
[image] 创建时间	2023/03/12
[image] **Description**	工具

VirusTotal是一个检查文件是否有病毒和恶意代码的服务，它发布了一个浏览器扩展，即VT4Browsers。

VT4Browsers 允许您发送一个下载的文件到该服务，并检查它是否有病毒。它是在浏览器中下载文件后自动完成的。通过点击扩展名图标，您可以获得有关该文件的信息。

有一些设置。例如，您可以在文件被VirusTotal扫描之前阻止它的打开。可以添加格式例外，如docx或pdf文件将不被发送扫描。该扩展可用于谷歌浏览器和火狐浏览器。

 https://chrome.google.com/webstore/detail/vt4browsers/efbjojhplkelaegfbieplglfidafgoka/related
 https://addons.mozilla.org/en-US/firefox/addon/vt4browsers/

[image]
[image]

移动网络浏览器绕过互联网审查

[image] 关键词	反封锁 移动设备
[image] 创建时间	2023/03/18
[image] **Description**	工具

CENO是一个移动网络浏览器，可以用来绕过互联网审查，帮助用户检索被封锁的网页。

 https://gitlab.com/censorship-no/ceno-browser

网站：https://censorship.no/en/index.html

F-droid: https://f-droid.org/packages/ie.equalit.ceno/

[image]
[image]

移动网络浏览器绕过互联网审查

[image]	关键词	反封锁 移动设备
[image]	创建时间	2023年3月18日
[image]	**Description**	工具

CENO是一个移动网络浏览器，可以用来绕过互联网审查，帮助用户检索被封锁的网页。

 https://gitlab.com/censorship-no/ceno-browser

网站：https://censorship.no/en/index.html

F-droid: https://f-droid.org/packages/ie.equalit.ceno/

[image]
[image]

安全打开陌生的缩短链接

[image] 关键词	URL 自助 预防性
[image] 创建时间	2023年3月20日
[image] **Description**	工具

URLCheck 应用用于帮您打开可疑的/缩短的链接。

- 开源
- URL Cleaner 和 URL Scanner 功能
- 主机检查器功能
- 无广告，无跟踪

 https://f-droid.org/packages/com.trianguloy.urlchecker/

[image]
[image]

安全打开陌生的缩短链接

[image] 关键词	URL 自助 预防性
[image] 创建时间	2023/03/20
[image] **Description**	工具

URLCheck 应用用于帮您打开可疑的/缩短的链接。

- 开源
- URL Cleaner 和 URL Scanner 功能
- 主机检查器功能
- 无广告，无跟踪

 https://f-droid.org/packages/com.trianguloy.urlchecker/

[image]
[image]

用于去中心化网络的自托管轻量级通信工具

[image] 关键词	IMs 加密 去中心化 自托管
[image] 创建时间	2023/03/21
[image] Description	工具

一个用于去中心化网络的自托管轻量级通信工具。

显著特点包括：

▫基于公私钥的身份（不绑定到任何区块链或托管域）。
▫联邦（不同节点上的账户可以通信）。
▫基于主题的线程（帖子按主题组织，而不是按联系人组织）。
▫轻量级（服务器运行于Raspberry Pi Zero v1.3）。
▫去中心化（应用程序和联络节点之间的直接通信）。
▫响应性强（在手机、平板电脑和PC上显示良好）。
以及更多。

 https://github.com/balzack/databag

 您可以在这里测试该项目：https://databag.coredb.org/#/create

[image]
[image]

用于去中心化网络的自托管轻量级通信工具

[image] 关键词	IMs 加密 去中心化 自托管
[image] 关联	[image]一系列安全的即时通信软件和服务
[image] 创建时间	2023年3月21日
[image] **Description**	工具

一个用于去中心化网络的自托管轻量级通信工具。

显著特点包括：

▫基于公私钥的身份（不绑定到任何区块链或托管域）。
▫联邦（不同节点上的账户可以通信）。
▫基于主题的线程（帖子按主题组织，而不是按联系人组织）。
▫轻量级（服务器运行于Raspberry Pi Zero v1.3）。
▫去中心化（应用程序和联络节点之间的直接通信）。
▫响应性强（在手机、平板电脑和PC上显示良好）。
以及更多。

 https://github.com/balzack/databag

 您可以在这里测试该项目：https://databag.coredb.org/#/create

[image]
[image]

设备间安全地同步剪贴板

[image] 关键词	传输安全 加密 电脑 移动设备
[image] 创建时间	2023年3月22日
[image] **Description**	工具

ClipCascade 是一款轻量级工具，可使用端到端加密技术在设备间自动同步剪贴板，安全有保障。

它适用于桌面系统（Windows、Linux）和移动设备（Android）。

 https://github.com/Sathvik-Rao/ClipCascade

[image]
[image]

设备间安全地同步剪贴板

[image]	关键词	传输安全 加密 电脑 移动设备
[image]	创建时间	2023/03/22
[image]	**Description**	工具

ClipCascade 是一款轻量级工具，可使用端到端加密技术在设备间自动同步剪贴板，安全有保障。

它适用于桌面系统（Windows、Linux）和移动设备（Android）。

 https://github.com/Sathvik-Rao/ClipCascade

[image]
[image]

成为自己的邮件服务提供商

[image]	关键词	电邮 自托管
[image]	创建时间	2023/04/12
[image]	**Description**	工具

1. Mail-in-a-Box 是一个开源应用，用于运行您自己的邮件服务器。它与强大的安卓邮件客户端K-9 Mail进行了整合。https://mailinabox.email/

1. mailcow:dockerized 是一个邮件服务器，部署在docker容器中，需要最小的配置。https://github.com/mailcow/mailcow-dockerized

1. docker Mailserver - 一个生产就绪的全栈但简单的容器化邮件服务器（SMTP、IMAP、LDAP、反垃圾邮件、防病毒等）。https://github.com/docker-mailserver/docker-mailserver

1. Mox - 全功能的安全、开源的邮件服务器。https://github.com/mjl-/mox

[image]
[image]

成为自己的邮件服务提供商

[image]	关键词	电邮 自托管
[image]	创建时间	2023年4月12日
[image]	**Description**	工具

1. Mail-in-a-Box 是一个开源应用，用于运行您自己的邮件服务器。它与强大的安卓邮件客户端K-9 Mail进行了整合。https://mailinabox.email/

1. mailcow:dockerized 是一个邮件服务器，部署在docker容器中，需要最小的配置。https://github.com/mailcow/mailcow-dockerized

1. docker Mailserver - 一个生产就绪的全栈但简单的容器化邮件服务器（SMTP、IMAP、LDAP、反垃圾邮件、防病毒等）。https://github.com/docker-mailserver/docker-mailserver

1. Mox - 全功能的安全、开源的邮件服务器。https://github.com/mjl-/mox

[image]
[image]

取证和反取证工具及资源

[image] 关键词	取证 对抗性思考方式 自检
[image] 创建时间	2023/05/13
[image] **Description**	工具

"反取证" 意味着：首先让他们找不到你，即便他们找到了，他们也无法证明你是他们要找的人。

1、Awesome-anti-forensic

 https://github.com/droberson/Awesome-anti-forensic

一个很强大的用于反取证和取证的工具和软件包，包括加密、隐写和任何改变属性的东西。

包括比如，

独立的启动映像，可安全擦除大多数计算机的硬盘。适用于批量或紧急数据销毁；
取证浏览器。Sleuth Kit 的 GUI；
离线 NT 密码编辑器-在 Windows NT SAM 用户数据库文件中重置密码；
各种清洁产品；
ELF加密工具；
还有用于取证的GNU数据恢复工具；
用于检查NTFS的工具；
facebook内存取证工具；

用于分析PDF文件的工具；
检测图像中隐写内容的工具；
用于安全删除的Unix工具；
还有流量解码器等……

2、WinLogs-Killer

 https://github.com/ScorpioTM/WinLogs-Killer

这个工具可以清除Windows保存的各种日志和历史文件。

现在它可以删除：

Windows 事件日志；
Windows 远程桌面的历史；
最近打开的文件。

3、emerg

 https://github.com/cedriczirtacic/emerg

lkm模块用于紧急启动二进制文件/脚本。

它总是在后台运行（从内核空间），当你输入 "秘密口令" 时，它将做任何指定的事。

它适用于标准终端（tty），而不是伪终端（pty）。

该模块有两个参数，一个是短语（注意这个），另一个是可执行文件的路径。

Phrase：输入这个短语将是触发器，所以要明智地选择。

Exec：可执行文件（这可以是一个二进制文件或一个脚本）。

4、Kaiser

 https://github.com/NtRaiseHardError/Kaiser

一个有趣的病毒，特点包括：无文件的持久性，攻击和反取证能力。

这个项目不是为了逃避反病毒检测而设计的。

恶意软件最有利的属性之一是生存能力，作为保持弹性和逃避安全解决方案检测的一种手段。
这种恶意软件的性质应包括其套件中的反取证能力，以保持其足迹最小，以及篡改系统和取证证据，以防止其被捕获和分析。

与无文件方法相结合，复杂的恶意软件能够在攻击系统的同时保持规避，避开多年来发展和完善的传统检测方法。

Kaiser概念验证恶意软件的设计是为了展示反取证和无文件功能的一个子集。这些功能包括无文件保存和二进制执行，以及反取证对策，即禁用事件日志服务，并主动阻止被感染的机器和自身被取证分析，以防止任何进一步的入侵调查。

5、Anti Forensics

 https://github.com/7h3pr0xy/Anti-Forensics

Anti-forensics 是在您的电脑上不留痕迹的艺术，它旨在与常见的取证工具作斗争，以防止在您的计算机上进行取证测试的任何渗透。

这是一篇关于取证保护方法的定义和适当调整的文章，值得一读。

基本的东西都讲到了，并且具有一些有趣的表述，于是也包含一些有趣的想法。

6、Metadata Remover

 https://github.com/Anish-M-code/Metadata-Remover

删除不需要的元数据就可以改善隐私。很简单吧。

一个简单的元数据删除工具，用于从图像和视频中删除元数据。用 C 和 Python3 开发。

Python版本支持音频和torrent文件。

7、Fishy

 https://github.com/dasec/fishy

fishy是一个用Python实现的基于文件系统的数据隐藏技术的工具包。

它收集了各种常见的利用方法，利用文件系统层上的现有数据结构，从常见的文件访问方法中隐藏数据。

这个工具包旨在教育人们了解与数据隐藏相关的既定反取证技术的概念。

fishy的设计目标之一是保持一个模块化结构。隔离层允许功能被封装起来。

8、Forensia

 https://github.com/PaulNorman01/Forensia

红队成员的反取证工具。减少有效载荷耗尽并增加检测倒计时。可用于测试您的事件响应/取证团队的能力。

能力包括：

卸载Sysmon驱动
根据古特曼算法粉碎文件
禁用USNJrnl
禁用prefetch
删除日志和禁用事件日志的工具
用户辅助更新时间禁用器
禁用访问时间
删除最近的项目
清除 shim 缓存
清除最近的文件缓存
清除Shell Bag
删除Windows Defender的隔离文件
熔化文件

9、Myool

 https://github.com/cle0n/myool

取证保护、隐写、数据渗漏。使用 AES-256 加密文件并将其隐藏在任何 PDF 文件中。

适用于 Windows 和 Linux 的 Python 版本的 myool 要快得多，因为它不会多次访问磁盘。

10、Awesome-memory-forensics

 https://github.com/digitalisx/awesome-memory-forensics

为DFIR策划的卓越的内存取证研究清单。

内存取证是对计算机内存转储的取证分析。其主要用途是调查复杂的计算机攻击，这些攻击足够隐蔽，不会在硬盘上留下数据。因此，必须对内存（RAM）进行取证信息分析。

11、Anti-forensic technologies

 https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/anti-forensic-techniques

这篇文章概述了反取证的方法和它们的工作原理。

比如改变时间戳、usnjrnl、改变日志系统中的元数据。

还有对USB的反取证，以及更多。

如果您对这个领域感兴趣的话，推荐阅读。

12、Anti Forensics

 https://github.com/cbranan/Anti-Forensics

一份研究显示了常用取证工具包的优势和劣势。

该研究报告分为以下几个部分：

对隐藏、改变和破坏数据的反取证工具的研究，流行的多合一取证工具包，以及对评估这些取证工具包的文档策略的研究。

13、Awesome-forensics-1

 https://github.com/rezaduty/awesome-forensics-1/

一个很丰富的取证资源： 近 300 个开源取证工具和 600 篇取证博客文章。

14、Lockwatcher

 https://github.com/ncatlin/lockwatcher

反取证监测软件： 寻找未经授权的访问迹象并清除密钥/关闭一切。

Lockwatcher是建立在这样的假设之上的：如果有人试图在您的电脑被锁住的时候使用您的电脑，他们就会试图获取您的实时数据，所以这些数据需要被销毁，并且使电脑无法访问。

它的工作方式是：

只要您不在电脑前，就会锁定电脑。
与被锁定的计算机进行交互会导致崩溃。
加密密钥从内存中被移除，计算机被关闭。

15、

forensictools 是一套专为数字取证设计的工具包。

部分工具包括：
▫exiftool，一个命令行应用程序和 Perl 库，用于读写元信息。
▫YARA，一款开源工具，用于对恶意软件样本进行识别和分类。
▫OfficeMalScanner，一款 Office 取证工具，用于扫描恶意软件痕迹。
▫SQLECmd，一款根据需要查找和处理 SQLite 文件的工具。

▫WinPrefetchView，一款小型工具，可读取存储在系统中的Prefetch文件。
▫WFA 可对 Windows 操作系统中使用的一些特殊文件进行解码和分析。
▫BrowsingHistoryView 是一款读取各种网络浏览器历史数据并在一个表格中显示所有内容的实用工具。

还有更多...

https://github.com/cristianzsh/forensictools
站点： https://cristian.sh/projects/forensictools.html

……

如果您错过了：

- 《如果您的手机被盗或被警察抢走...》 https://iyouport.substack.com/p/a5e

- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》 https://iyouport.substack.com/p/iphone-d80

- 《如何让您的 iPhone 能够防小偷》 https://iyouport.substack.com/p/-iphone--a57
  -《如何保持 Android 设备免受警察的侵害》 https://iyouport.substack.com/p/-android-

以及：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》https://iyouport.substack.com/p/26c?s=w
  -《警察查手机的东西长什么样？-- 从技术角度看移动设备取证》https://iyouport.substack.com/p/--4f1?s=w

-《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
https://iyouport.substack.com/p/lr--155
-《警察有可能如何恢复您已删除的互联网浏览历史记录》
https://iyouport.substack.com/p/694?s=w

[image]
[image]

取证和反取证工具及资源

[image]	关键词	取证 对抗性思考方式 自检
[image]	创建时间	2023年5月13日
[image]	**Description**	工具

"反取证" 意味着：首先让他们找不到你，即便他们找到了，他们也无法证明你是他们要找的人。

1、Awesome-anti-forensic

 https://github.com/droberson/Awesome-anti-forensic

一个很强大的用于反取证和取证的工具和软件包，包括加密、隐写和任何改变属性的东西。

包括比如，

独立的启动映像，可安全擦除大多数计算机的硬盘。适用于批量或紧急数据销毁；
取证浏览器。Sleuth Kit 的 GUI；
离线 NT 密码编辑器-在 Windows NT SAM 用户数据库文件中重置密码；
各种清洁产品；
ELF加密工具；
还有用于取证的GNU数据恢复工具；
用于检查NTFS的工具；
facebook内存取证工具；

用于分析PDF文件的工具；
检测图像中隐写内容的工具；
用于安全删除的Unix工具；
还有流量解码器等……

2、WinLogs-Killer

 https://github.com/ScorpioTM/WinLogs-Killer

这个工具可以清除Windows保存的各种日志和历史文件。

现在它可以删除：

Windows 事件日志；
Windows 远程桌面的历史；
最近打开的文件。

3、emerg

 https://github.com/cedriczirtacic/emerg

lkm模块用于紧急启动二进制文件/脚本。

它总是在后台运行（从内核空间），当你输入 "秘密口令" 时，它将做任何指定的事。

它适用于标准终端（tty），而不是伪终端（pty）。

该模块有两个参数，一个是短语（注意这个），另一个是可执行文件的路径。

Phrase：输入这个短语将是触发器，所以要明智地选择。

Exec：可执行文件（这可以是一个二进制文件或一个脚本）。

4、Kaiser

 https://github.com/NtRaiseHardError/Kaiser

一个有趣的病毒，特点包括：无文件的持久性，攻击和反取证能力。

这个项目不是为了逃避反病毒检测而设计的。

恶意软件最有利的属性之一是生存能力，作为保持弹性和逃避安全解决方案检测的一种手段。
这种恶意软件的性质应包括其套件中的反取证能力，以保持其足迹最小，以及篡改系统和取证证据，以防止其被捕获和分析。

与无文件方法相结合，复杂的恶意软件能够在攻击系统的同时保持规避，避开多年来发展和完善的传统检测方法。

Kaiser概念验证恶意软件的设计是为了展示反取证和无文件功能的一个子集。这些功能包括无文件保存和二进制执行，以及反取证对策，即禁用事件日志服务，并主动阻止被感染的机器和自身被取证分析，以防止任何进一步的入侵调查。

5、Anti Forensics

 https://github.com/7h3pr0xy/Anti-Forensics

Anti-forensics 是在您的电脑上不留痕迹的艺术，它旨在与常见的取证工具作斗争，以防止在您的计算机上进行取证测试的任何渗透。

这是一篇关于取证保护方法的定义和适当调整的文章，值得一读。

基本的东西都讲到了，并且具有一些有趣的表述，于是也包含一些有趣的想法。

6、Metadata Remover

https://github.com/Anish-M-code/Metadata-Remover

删除不需要的元数据就可以改善隐私。很简单吧。

一个简单的元数据删除工具，用于从图像和视频中删除元数据。用 C 和 Python3 开发。

Python版本支持音频和torrent文件。

7、Fishy

https://github.com/dasec/fishy

fishy是一个用Python实现的基于文件系统的数据隐藏技术的工具包。

它收集了各种常见的利用方法，利用文件系统层上的现有数据结构，从常见的文件访问方法中隐藏数据。

这个工具包旨在教育人们了解与数据隐藏相关的既定反取证技术的概念。

fishy的设计目标之一是保持一个模块化结构。隔离层允许功能被封装起来。

8、Forensia

 https://github.com/PaulNorman01/Forensia

红队成员的反取证工具。减少有效载荷耗尽并增加检测倒计时。可用于测试您的事件响应/取证团队的能力。

能力包括：

卸载Sysmon驱动
根据古特曼算法粉碎文件
禁用USNJrnl
禁用prefetch
删除日志和禁用事件日志的工具
用户辅助更新时间禁用器
禁用访问时间
删除最近的项目
清除 shim 缓存
清除最近的文件缓存
清除Shell Bag
删除Windows Defender的隔离文件
熔化文件

9、Myool

 https://github.com/cle0n/myool

取证保护、隐写、数据渗漏。使用 AES-256 加密文件并将其隐藏在任何 PDF 文件中。

适用于 Windows 和 Linux 的 Python 版本的 myool 要快得多，因为它不会多次访问磁盘。

10、Awesome-memory-forensics

 https://github.com/digitalisx/awesome-memory-forensics

为DFIR策划的卓越的内存取证研究清单。

内存取证是对计算机内存转储的取证分析。其主要用途是调查复杂的计算机攻击，这些攻击足够隐蔽，不会在硬盘上留下数据。因此，必须对内存（RAM）进行取证信息分析。

11、Anti-forensic technologies

□ https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/anti-forensic-techniques

这篇文章概述了反取证的方法和它们的工作原理。

比如改变时间戳、usnjrnl、改变日志系统中的元数据。

还有对USB的反取证，以及更多。

如果您对这个领域感兴趣的话，推荐阅读。

12、Anti Forensics

□ https://github.com/cbranan/Anti-Forensics

一份研究显示了常用取证工具包的优势和劣势。

该研究报告分为以下几个部分：

对隐藏、改变和破坏数据的反取证工具的研究，流行的多合一取证工具包，以及对评估这些取证工具包的文档策略的研究。

13、Awesome-forensics-1

https://github.com/rezaduty/awesome-forensics-1/

一个很丰富的取证资源： 近 300 个开源取证工具和 600 篇取证博客文章。

14、Lockwatcher

https://github.com/ncatlin/lockwatcher

反取证监测软件： 寻找未经授权的访问迹象并清除密钥/关闭一切。

Lockwatcher是建立在这样的假设之上的：如果有人试图在您的电脑被锁住的时候使用您的电脑，他们就会试图获取您的实时数据，所以这些数据需要被销毁，并且使电脑无法访问。

它的工作方式是：

只要您不在电脑前，就会锁定电脑。
与被锁定的计算机进行交互会导致崩溃。
加密密钥从内存中被移除，计算机被关闭。

15、

forensictools 是一套专为数字取证设计的工具包。

部分工具包括：
▫ exiftool，一个命令行应用程序和 Perl 库，用于读写元信息。
▫ YARA，一款开源工具，用于对恶意软件样本进行识别和分类。
▫ OfficeMalScanner，一款 Office 取证工具，用于扫描恶意软件痕迹。
▫ SQLECmd，一款根据需要查找和处理 SQLite 文件的工具。

▫WinPrefetchView，一款小型工具，可读取存储在系统中的Prefetch文件。
▫WFA 可对 Windows 操作系统中使用的一些特殊文件进行解码和分析。
▫BrowsingHistoryView 是一款读取各种网络浏览器历史数据并在一个表格中显示所有内容的实用工具。

还有更多...

https://github.com/cristianzsh/forensictools
站点： https://cristian.sh/projects/forensictools.html

……

如果您错过了：

- 《如果您的手机被盗或被警察抢走…》 https://iyouport.substack.com/p/a5e

- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》 https://iyouport.substack.com/p/iphone-d80

- 《如何让您的 iPhone 能够防小偷》 https://iyouport.substack.com/p/-iphone--a57
  -《如何保持 Android 设备免受警察的侵害》 https://iyouport.substack.com/p/-android-

以及：

- 《数字取证正在泛滥：政府可以从你的手机中提取哪些数据？》https://iyouport.substack.com/p/26c?s=w
  -《警察查手机的东西长什么样？-- 从技术角度看移动设备取证》https://iyouport.substack.com/p/--4f1?s=w

-《让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证》
https://iyouport.substack.com/p/lr--155
-《警察有可能如何恢复您已删除的互联网浏览历史记录》
https://iyouport.substack.com/p/694?s=w

[image]
[image]

对URL进行加密和解密

[image] 关键词	URL 传输安全 加密
[image] 创建时间	2023/05/26
[image] **Description**	工具

Link Lock 是一个对URL进行加密和解密的工具。

当用户访问一个加密的URL时，他们会被提示输入密码。如果密码正确，Link Lock 会检索原始URL，然后将其重定向到那里。否则将显示错误。用户还可以添加提示。

每个加密的URL都完全存储在应用程序创建的链接中。因此，用户可以控制他们用Link Lock创建的所有数据。没有任何东西被储存在服务器上，没有cookies、没有跟踪、无需注册。

Link Lock 有许多用途，比如：
▫ 在共享计算机上存储私人书签
▫ 加密整个网页（通过URL Pages）。
▫ 通过公开的或不安全的渠道发送敏感链接（例如，发布需要密码才能访问的网站的链接）
▫ 为共享的 Dropbox 或 Google 云端硬盘链接添加密码
▫ 共享受密码保护的磁力链接和种子

一切都在你的浏览器中运行。

 https://github.com/jstrieb/link-lock

网站：https://jstrieb.github.io/link-lock/create/

[image]
[image]

对URL进行加密和解密

[image] 关键词	URL 传输安全 加密
[image] 创建时间	2023年5月26日
[image] **Description**	工具

Link Lock 是一个对URL进行加密和解密的工具。

当用户访问一个加密的URL时，他们会被提示输入密码。如果密码正确，Link Lock 会检索原始URL，然后将其重定向到那里。否则将显示错误。用户还可以添加提示。

每个加密的URL都完全存储在应用程序创建的链接中。因此，用户可以控制他们用Link Lock创建的所有数据。没有任何东西被储存在服务器上，没有cookies、没有跟踪、无需注册。

Link Lock 有许多用途，比如：
▫ 在共享计算机上存储私人书签
▫ 加密整个网页（通过URL Pages）。
▫ 通过公开的或不安全的渠道发送敏感链接（例如，发布需要密码才能访问的网站的链接）
▫ 为共享的 Dropbox 或 Google 云端硬盘链接添加密码
▫ 共享受密码保护的磁力链接和种子

一切都在你的浏览器中运行。

 https://github.com/jstrieb/link-lock

网站：https://jstrieb.github.io/link-lock/create/

[image]
[image]

安全搜索

[image] 关键词	元搜索 免追踪 安全搜索
[image] 创建时间	2023/05/31
[image] **Description**	工具

izito是一个值得信赖的谷歌搜索引擎的替代品。它结合了多个搜索引擎：雅虎、微软必应、YouTube、Wikipedia、Entireweb和其他 ... 使用dorks。

 https://www.izito.com/

[image]
[image]

安全搜索

[image] 关键词	元搜索 免追踪 安全搜索
[image] 创建时间	2023年5月31日
[image] **Description**	工具

izito是一个值得信赖的谷歌搜索引擎的替代品。它结合了多个搜索引擎：雅虎、微软必应、YouTube、Wikipedia、Entireweb和其他 ... 使用dorks。

 https://www.izito.com/

[image]
[image]

提高安卓设备隐私和性能的工具

[image] 关键词	反封锁 安卓 沙箱
[image] 创建时间	2023年6月19日
[image] **Description**	工具

1. Island - 是一个沙盒，允许您将选定的应用程序在隔离状态下运行，防止这些应用访问您的个人数据或设备信息。包括比如仅在一侧使用VPN，或在两侧使用不同的VPN。

1. SuperFreezZ - 一个允许您冻结其他应用程序的所有后台活动的应用。结合离线模式，可以增加您的智能手机的电池寿命。

[image]
[image]

提高安卓设备隐私和性能的工具

[image] 关键词	反封锁 安卓 沙箱
[image] 创建时间	2023/06/19
[image] **Description**	工具

1. Island - 是一个沙盒，允许您将选定的应用程序在隔离状态下运行，防止这些应用访问您的个人数据或设备信息。包括比如仅在一侧使用VPN，或在两侧使用不同的VPN。

1. SuperFreezZ - 一个允许您冻结其他应用程序的所有后台活动的应用。结合离线模式，可以增加您的智能手机的电池寿命。

[image]
[image]

创建个人VPN

[image]	关键词	代理 反审查 反封锁 自助
[image]	创建时间	2023年6月21日
[image]	**Description**	工具

MyVPN是一个用于创建个人VPN服务器的应用程序。L2TP、PPTP、OpenVPN、WireGuard等。供应商：DigitalOcean, Linode, CryptoServers, Hetzner Cloud

 https://github.com/my0419/myvpn-desktop

[image]
[image]

创建个人VPN

[image] 关键词	代理 反审查 反封锁 自助
[image] 创建时间	2023/06/21
[image] **Description**	工具

MyVPN是一个用于创建个人VPN服务器的应用程序。L2TP、PPTP、OpenVPN、WireGuard等。供应商：DigitalOcean, Linode, CryptoServers, Hetzner Cloud

 https://github.com/my0419/myvpn-desktop

[image]
[image]

安全的即时通信工具 Speek

[image]	关键词	IMs 免追踪 加密 去中心化
[image]	创建时间	2023年6月22日
[image]	**Description**	工具

即时通信工具 Speek 无服务器、不存储元数据，不需要电话号码，所有信息包括文件传输都是端对端加密的，并通过Tor网络传输。这此外，由于其去中心化（p2p）的性质，没有任何中间人服务器可能被破坏，被拿下或泄露用户信息，如IP地址、联系人、元数据甚至消息。

用户只通过公钥进行识别。每个用户都可以与其他人分享自己的公钥，将彼此加入到联系人名单中。

- 可以在不向任何人暴露您的身份（或IP地址）的情况下聊天；
- 没有人可以发现您的联系人是谁或你们什么时候说的话（无元数据）
- 您的信息和数据永远不会存储在任何服务器上，可以在没有中间人的情况下进行交谈；
- 没有任何服务器或运营商可能被破坏、暴露您的信息；
- 跨平台，对非技术用户友好；
- 您所有的信息都是私人的。没有任何东西被储存，也没有任何元数据。一旦您关闭Speek 所有信息都会被删除。

 https://speek.network/

[image]
[image]

安全的即时通信工具 Speek

[image] 关键词	IMs 免追踪 加密 去中心化
[image] 创建时间	2023/06/22
[image] **Description**	工具

即时通信工具 Speek 无服务器、不存储元数据，不需要电话号码，所有信息包括文件传输都是端对端加密的，并通过Tor网络传输。这此外，由于其去中心化（p2p）的性质，没有任何中间人服务器可能被破坏，被拿下或泄露用户信息，如IP地址、联系人、元数据甚至消息。

用户只通过公钥进行识别。每个用户都可以与其他人分享自己的公钥，将彼此加入到联系人名单中。

- 可以在不向任何人暴露您的身份（或IP地址）的情况下聊天；
- 没有人可以发现您的联系人是谁或你们什么时候说的话（无元数据）
- 您的信息和数据永远不会存储在任何服务器上，可以在没有中间人的情况下进行交谈；
- 没有任何服务器或运营商可能被破坏、暴露您的信息；
- 跨平台，对非技术用户友好；
- 您所有的信息都是私人的。没有任何东西被储存，也没有任何元数据。一旦您关闭Speek 所有信息都会被删除。

□ https://speek.network/

[image]
[image]

在不安全的渠道上安全传输

[image] 关键词	传输安全 免追踪 反审查
[image] 创建时间	2023年7月3日
[image] **Description**	工具

Portable Secret 是一个小技巧，它允许您：

- 通过不安全的渠道（如电子邮件、短信等）发送加密的消息/图像/文件；
- 将敏感信息（如密码、文档、私钥、2FA 恢复代码等）存储在不安全的位置（如网络、云、USB 驱动器等处）

它是便携的，因为解密这些秘密不需要任何特殊的软件 —— 您只需要一个浏览器。

它适合那些需要足够的安全性但无法使用PGP, age等工具的人。

它只是一个HTML 文件任何现代的网络浏览器都可以打开它，即使没有互联网连接也没问题；知道密码的人才能解密。

这有一个例子您可以试试（密码是 banana）：https://mprimi.github.io/portable-secret/examples/example-message.html

该文件是独立的，没有外部依赖项。它可以放在USB驱动器上携带，并在没有互联网连接的情况下在任何具有网络浏览器的设备上解密。

https://www.privacyprotect.dev/

还有其他类似的保密工具，比如：
这个：https://github.com/jwillmer/emergency-contacts
这个：https://github.com/kaushalmeena/digi-cloak
还有这个：https://github.com/robinmoisson/staticrypt
或者这个：https://9p4.github.io/hackna/
以及这个：https://github.com/dividuum/html-vault
还有更多：https://prettyeasyprivacy.xyz/

[image]
[image]

在不安全的渠道上安全传输

[image]	关键词	传输安全 免追踪 反审查
[image]	创建时间	2023/07/03
[image]	**Description**	工具

Portable Secret 是一个小技巧，它允许您：

- 通过不安全的渠道（如电子邮件、短信等）发送加密的消息/图像/文件；
- 将敏感信息（如密码、文档、私钥、2FA 恢复代码等）存储在不安全的位置（如网络、云、USB 驱动器等处）

它是便携的，因为解密这些秘密不需要任何特殊的软件 —— 您只需要一个浏览器。

它适合那些需要足够的安全性但无法使用PGP, age等工具的人。

它只是一个HTML 文件任何现代的网络浏览器都可以打开它，即使没有互联网连接也没问题；知道密码的人才能解密。

这有一个例子您可以试试（密码是 banana）：https://mprimi.github.io/portable-secret/examples/example-message.html

该文件是独立的，没有外部依赖项。它可以放在USB驱动器上携带，并在没有互联网连接的情况下在任何具有网络浏览器的设备上解密。

https://www.privacyprotect.dev/

还有其他类似的保密工具，比如：
这个：https://github.com/jwillmer/emergency-contacts
这个：https://github.com/kaushalmeena/digi-cloak
还有这个：https://github.com/robinmoisson/staticrypt
或者这个：https://9p4.github.io/hackna/
以及这个：https://github.com/dividuum/html-vault
还有更多：https://prettyeasyprivacy.xyz/

[image]
[image]

离线安全传输

[image] 关键词	传输安全
[image] 创建时间	2023/07/04
[image] **Description**	工具

LocalSend - 另一个用于与相邻设备传输文件的应用程序。

免费、开源、跨平台。不需要互联网连接，也不需要外部服务器。该应用程序允许您在本地局域网上发送文件和信息。

 https://github.com/localsend/localsend

F-droid: https://f-droid.org/packages/org.localsend.localsend_app/

网站：https://localsend.org/

[image]
[image]

离线安全传输

[image]	关键词	传输安全
[image]	创建时间	2023年7月4日
[image]	**Description**	工具

LocalSend - 另一个用于与相邻设备传输文件的应用程序。

免费、开源、跨平台。不需要互联网连接，也不需要外部服务器。该应用程序允许您在本地局域网上发送文件和信息。

 https://github.com/localsend/localsend

F-droid: https://f-droid.org/packages/org.localsend.localsend_app/

网站：https://localsend.org/

[image]
[image]

一个功能强大的自托管 Internet 存档解决方案

[image] 关键词	文件处理 查询整理 自托管
[image] 创建时间	2023/07/17
[image] **Description**	工具

ArchiveBox是一个自托管的本地网络档案。允许您保存网页内容、浏览器历史记录中的来源、书签、资源库，并以各种形式保存，从通常的html、js和PDF到各种媒体格式的音频、视频上传等形式。支持在自动模式下工作，还允许您在内容源变化时发送通知。

 http://archivebox.io/

[image]
[image]

一个功能强大的自托管 Internet 存档解决方案

[image] 关键词	文件处理 查询整理 自托管
[image] 关联	[image]随手存档 ；[image]交互式高质量网页存档
[image] 创建时间	2023年7月17日
[image] **Description**	工具

ArchiveBox是一个自托管的本地网络档案。允许您保存网页内容、浏览器历史记录中的来源、书签、资源库，并以各种形式保存，从通常的html、js和PDF到各种媒体格式的音频、视频上传等形式。支持在自动模式下工作，还允许您在内容源变化时发送通知。

 http://archivebox.io/

[image]
[image]

通用安卓卸载器GUI

[image] 关键词	安卓 清理
[image] 创建时间	2023年7月18日
[image] **Description**	工具

一个用Rust编写的跨平台GUI，使用ADB来卸载、冻结、禁用和重新安Android设备的系统应用。

其目的是通过移除不必要的和难以理解的系统应用来改善隐私和电池性能。这也可以通过减少攻击面来帮助提高安全性。

 https://github.com/0x192/universal-android-debloater

[image]
[image]

通用安卓卸载器GUI

[image] 关键词	安卓 清理
[image] 创建时间	2023/07/18
[image] **Description**	工具

一个用Rust编写的跨平台GUI，使用ADB来卸载、冻结、禁用和重新安Android设备的系统应用。

其目的是通过移除不必要的和难以理解的系统应用来改善隐私和电池性能。这也可以通过减少攻击面来帮助提高安全性。

 https://github.com/0x192/universal-android-debloater

[image]
[image]

点对点的匿名安全通信

[image] 关键词	IMs P2P tor
[image] 创建时间	2023年8月8日
[image] **Description**	工具

AnonymousMessenger - 一个点对点的匿名安全通信工具，通过 tor 工作。自由开源软件。 所有数据仅存储在您的设备上。

 https://www.anonymousmessenger.ly/

[image]
[image]

点对点的匿名安全通信

[image] 关键词	IMs P2P tor
[image] 创建时间	2023/08/08
[image] **Description**	工具

AnonymousMessenger - 一个点对点的匿名安全通信工具，通过 tor 工作。自由开源软件。 所有数据仅存储在您的设备上。

 https://www.anonymousmessenger.ly/

[image]
[image]

自动检测链接是否安全

[image] 关键词	URL 病毒检测 预防性
[image] 创建时间	2023年8月10日
[image] **Description**	工具

Quad9 是一种资源，其目的是保护用户免受恶意软件和网络钓鱼的侵害。

每当 Quad9 用户点击一个网站链接或在网络浏览器中输入一个地址，Quad9 就会根据从19个不同的威胁情报合作伙伴汇总的域名列表检查该网站。

 https://quad9.net/

[image]
[image]

自动检测链接是否安全

[image] 关键词	URL 病毒检测 预防性
[image] 创建时间	2023/08/10
[image] **Description**	工具

Quad9 是一种资源，其目的是保护用户免受恶意软件和网络钓鱼的侵害。

每当 Quad9 用户点击一个网站链接或在网络浏览器中输入一个地址，Quad9 就会根据从19个不同的威胁情报合作伙伴汇总的域名列表检查该网站。

 https://quad9.net/

[image]
[image]

Telegram探索工具

[image] 关键词	OSINT telegram 安全搜索
[image] 关联	[image]Telegram内容提取工具；[image]Telegram 语音笔记转录和摘要机器人；[image]Telegram探索工具
[image] 创建时间	2023年9月12日
[image] **Description**	工具

1. Lyzem (https://lyzem.com/) 一个搜索引擎，用于搜索开放的聊天、频道、Telegram机器人和telegra.ph 页面。

1. TeleGaGo (https://cse.google.com.hk/cse?cx=006368593537057042503:efxu7xprihg#gsc.tab=0) - Telegram的谷歌自定义搜索。

1. Intelligence X (https://intelx.io/tools?tab=telegram)- 著名搜索引擎不需要更多介绍。建议用Tor。

1. Telegram Tracker (https://github.com/estebanpdl/telegram-tracker)- 连接到 Telegram API 并生成任何频道（包括媒体和帖子）的JSON文件（备份）。

1. Tgdev (https://tgdev.io/tme/) - 通过关键字搜索 Telegram 频道和帖子。

1. Telegram Search Engine (https://chrome.google.com/

webstore/detail/tg-search-engine-tg-group/
ilpgiemienkecbgdhdbgdjkafodgfojl)- 用于搜集Telegram 频道和群组链接的扩展。

[image]
[image]

Telegram探索工具

[image] 关键词	OSINT telegram 安全搜索
[image] 创建时间	2023/09/12
[image] **Description**	工具

1. Lyzem (https://lyzem.com/) 一个搜索引擎，用于搜索开放的聊天、频道、Telegram机器人和telegra.ph 页面。

1. TeleGaGo (https://cse.google.com.hk/cse?cx=006368593537057042503:efxu7xprihg#gsc.tab=0) - Telegram的谷歌自定义搜索。

1. Intelligence X (https://intelx.io/tools?tab=telegram)- 著名搜索引擎不需要更多介绍。建议用Tor。

1. Telegram Tracker (https://github.com/estebanpdl/telegram-tracker)- 连接到 Telegram API 并生成任何频道（包括媒体和帖子）的JSON文件（备份）。

1. Tgdev (https://tgdev.io/tme/) - 通过关键字搜索 Telegram 频道和帖子。

1. Telegram Search Engine (https://chrome.google.com/webstore/detail/tg-search-engine-tg-group/ilpgiemienkecbgdhdbgdjkafodgfojl)- 用于搜集Telegram 频道和群组链接的扩展。

[image]
[image]

一次性加密笔记

[image] 关键词	传输安全 加密 阅后即焚
[image] 创建时间	2023/09/21
[image] **Description**	工具

Ghost Secret - 自动销毁的一次性加密笔记服务。允许您设置信息的寿命，以天数或被查阅次数为单位。

 https://secret.ghostbyjohnmcafee.com/

[image]
[image]

一次性加密笔记

[image] 关键词	传输安全 加密 阅后即焚
[image] 创建时间	2023年9月21日
[image] **Description**	工具

Ghost Secret - 自动销毁的一次性加密笔记服务。允许您设置信息的寿命，以天数或被查阅次数为单位。

 https://secret.ghostbyjohnmcafee.com/

[image]
[image]

将整个网站转换为PDF

[image] 关键词	反封锁 查询整理
[image] 创建时间	2023/09/22
[image] **Description**	工具

PDF my URL 允许您下载一个PDF格式的网站，以供离线查看。

您可以将单个页面或整个网站转换为PDF，并保持匿名（该应用程序的IP地址从网站上请求信息，而不是您的IP）。

 https://pdfmyurl.com/

[image]
[image]

将整个网站转换为PDF

[image] 关键词	反封锁 查询整理
[image] 创建时间	2023年9月22日
[image] **Description**	工具

PDF my URL 允许您下载一个PDF格式的网站，以供离线查看。

您可以将单个页面或整个网站转换为PDF，并保持匿名（该应用程序的IP地址从网站上请求信息，而不是您的IP）。

 https://pdfmyurl.com/

[image]
[image]

安全浏览器

[image]	关键词	代理 免追踪 反封锁 反间谍 数字足迹 预防性
[image]	创建时间	2023/10/17
[image]	**Description**	工具

Mullvad 浏览器是一款专为网络安全和匿名工作设计的免费的浏览器。Mullvad VPN团队开发。包含保护您的在线活动所需的所有基本功能。

该浏览器可以说是一个没有Tor网络的Tor浏览器。您可以使用值得信赖的VPN进行保护。这个想法是为了提供除了Tor网之外的另一种选择。 让您可以以更多的隐私浏览互联网。帮助尽可能多的人对抗大数据。

该浏览器支持 "不留痕迹"模式，不仅能在您关闭浏览器后删除所有在线活动痕迹，还能阻止网站和广告对您的任何追踪。

 https://mullvad.net/en/browser

https://iyouport.substack.com/p/lr--67d?utm_source=publication-search

[image]
[image]

安全浏览器

[image]	关键词	代理 免追踪 反封锁 反间谍 数字足迹 预防性
[image]	创建时间	2023年10月17日
[image]	**Description**	工具

Mullvad 浏览器是一款专为网络安全和匿名工作设计的免费的浏览器。Mullvad VPN团队开发。包含保护您的在线活动所需的所有基本功能。

该浏览器可以说是一个没有Tor网络的Tor浏览器。您可以使用值得信赖的VPN进行保护。这个想法是为了提供除了Tor网之外的另一种选择。 让您可以以更多的隐私浏览互联网。帮助尽可能多的人对抗大数据。

该浏览器支持 "不留痕迹"模式，不仅能在您关闭浏览器后删除所有在线活动痕迹，还能阻止网站和广告对您的任何追踪。

 https://mullvad.net/en/browser

https://iyouport.substack.com/p/lr--67d?utm_source=publication-search

[image]
[image]

无限制传输任何大小的文件

[image] 关键词	P2P 传输安全
[image] 创建时间	2023年10月19日
[image] **Description**	工具

如果您不想忍受长时间的下载，而您需要传送的文件又很大，那么不妨试试 ToffeeShare。这不仅仅是另一种云存储服务，它采用 P2P 工作原理，即直接将您的数据传输给接收方，就像 torrent 客户端那样。

传输文件的大小和下载速度都不受限制。一切都只取决于网速 —— 您和接收方的网速。操作原理非常简单：点击 ToffeeShare 页面中间的大圆按钮，选择想要的文件。或者直接将文件拖入浏览器窗口。

服务会生成一个链接，并提供将其复制到剪贴板或通过社交网络发送的功能。当接收方打开链接时，只需下载文件即可。

 https://toffeeshare.com/

[image]
[image]

无限制传输任何大小的文件

[image] 关键词	P2P 传输安全
[image] 创建时间	2023/10/19
[image] **Description**	工具

如果您不想忍受长时间的下载，而您需要传送的文件又很大，那么不妨试试 ToffeeShare。这不仅仅是另一种云存储服务，它采用 P2P 工作原理，即直接将您的数据传输给接收方，就像 torrent 客户端那样。

传输文件的大小和下载速度都不受限制。一切都只取决于网速 —— 您和接收方的网速。操作原理非常简单：点击 ToffeeShare 页面中间的大圆按钮，选择想要的文件。或者直接将文件拖入浏览器窗口。

服务会生成一个链接，并提供将其复制到剪贴板或通过社交网络发送的功能。当接收方打开链接时，只需下载文件即可。

 https://toffeeshare.com/

[image]
[image]

将手机变成电脑麦克风

[image]	关键词	电脑 移动设备
[image]	创建时间	2023年10月20日
[image]	**Description**	工具

每个人都有麦克风坏了需要更换的时候，Wo Mic应用程序可以将您的手机用作麦克风使用。

为此，您需要：

1. 下载 Android 或 iOS 版 Wo Mic 应用程序，并将其安装到电脑上。

1. 然后打开智能手机上的应用设置，选择连接方式。

1. 返回主菜单并按 "Play"。

1. 在电脑上启动应用程序，转到 "连接"部分并按 "连接"。

1. 输入智能手机应用程序中的 IP 地址。

 https://wolicheng.com/womic/

 安卓：https://play.google.com/store/apps/details?id=com.wo.voice2&pli=1

 iOS：https://apps.apple.com/us/app/id1260978417

[image]
[image]

将手机变成电脑麦克风

[image]	关键词	电脑 移动设备
[image]	创建时间	2023/10/20
[image]	**Description**	工具

每个人都有麦克风坏了需要更换的时候，Wo Mic应用程序可以将您的手机用作麦克风使用。

为此，您需要：

1. 下载 Android 或 iOS 版 Wo Mic 应用程序，并将其安装到电脑上。

1. 然后打开智能手机上的应用设置，选择连接方式。

1. 返回主菜单并按 "Play"。

1. 在电脑上启动应用程序，转到 "连接"部分并按 "连接"。

1. 输入智能手机应用程序中的 IP 地址。

 https://wolicheng.com/womic/

 安卓：https://play.google.com/store/apps/details?id=com.wo.voice2&pli=1

 iOS：https://apps.apple.com/us/app/id1260978417

[image]
[image]

保护安卓手机免受警察的抢夺

[image]	关键词	反侦察 安卓 移动设备 自助 防御 预防性
[image]	创建时间	2023/10/26
[image]	**Description**	工具

以下仅限 Android 设备和紧急按钮的选项，无需root。

1. Data Wipe Screen Locker (https://m.apkpure.com/data-wipe-screen-locker/com.safetyjabber.datawipe)是一款专门为紧急情况设计的应用程序，让您可以以最快的方式销毁手机中的数据。输入提前设置好的特殊的PIN码即可销毁所有数据。可为应用程序设置密码。完全免费。

1. Wasted (https://f-droid.org/packages/me.lucky.wasted/)以前介绍过了，这是一款在危险情况下可以让您锁定设备并删除数据的应用程序。您可以使用紧急按钮、快速设置或发送带有验证码的消息。

1. App Lock (https://play.google.com/store/apps/details?id=com.thinkyeah.smartlockfree&hl=en) 用密码或锁保护已安装的应用程序，并防止在运行您指定的应用程序时关闭屏幕或切换到横屏模式。

1. Duress (https://f-droid.org/packages/me.lucky.duress/) 可以让您在锁屏界面上设置胁迫密码的应用程序。其原理是，当您在手机上输入这个密码时，可以悄悄向预定的联系人发送一条紧急求救信息。新版本有中文。

[image]
[image]

保护安卓手机免受警察的抢夺

[image] 关键词	反侦察 安卓 移动设备 自助 防御 预防性
[image] 创建时间	2023年10月26日
[image] **Description**	工具

以下仅限 Android 设备和紧急按钮的选项，无需root。

1. Data Wipe Screen Locker (https://m.apkpure.com/data-wipe-screen-locker/com.safetyjabber.datawipe)是一款专门为紧急情况设计的应用程序，让您可以以最快的方式销毁手机中的数据。输入提前设置好的特殊的PIN码即可销毁所有数据。可为应用程序设置密码。完全免费。

1. Wasted (https://f-droid.org/packages/me.lucky.wasted/)以前介绍过了，这是一款在危险情况下可以让您锁定设备并删除数据的应用程序。您可以使用紧急按钮、快速设置或发送带有验证码的消息。

1. App Lock (https://play.google.com/store/apps/details?id=com.thinkyeah.smartlockfree&hl=en) 用密码或锁保护已安装的应用程序，并防止在运行您指定的应用程序时关闭屏幕或切换到横屏模式。

1. Duress (https://f-droid.org/packages/me.lucky.duress/) 可以让您在锁屏界面上设置胁迫密码的应用程序。其原理是，当您在手机上输入这个密码时，可以悄悄向预定的联系人发送一条紧急求救信息。新版本有中文。

[image]
[image]

Tor工具系列

[image] 关键词	tor 反封锁 安全搜索 暗网
[image] 创建时间	2023/11/06
[image] **Description**	工具

1. TOR Node List (https://www.dan.me.uk/tornodes) - 节点列表；

1. Onionite (https://github.com/lukechilds/onionite) - 有关节点的信息；

1. Tor Metrics (https://metrics.torproject.org/) - 节点信息；

1. TorBot (https://github.com/DedSecInside/TorBot) 是一款用Python编写的智能开源情报工具。

1. OnionBot (https://github.com/Flobin/OnionBot) 是一款以twitter机器人形式实现的.onion网站爬虫。

1. OnionScan (https://github.com/s-rah/onionscan) - 另一款优秀的洋葱网站爬虫。

1. VililantOnion (https://github.com/andreyglauzer/VigilantOnion) - 通过关键字进行搜索的爬虫。

1. OnionIngestor (https://github.com/danieleperera/

OnionIngestor) - 用于收集和抓取.onion 网站并将收集到的信息编入 Elasticsearch 索引的工具。

1. Darkus (https://github.com/Lucksi/Darkus) 是一款使用关键字的洋葱网站搜索引擎。

暗网开源情报Full Pack

1. 网络信息
   TOR Node List (https://www.dan.me.uk/tornodes) - 节点列表；
   ExoneraTor (https://metrics.torproject.org/exonerator.html) - 检查IP是否用作Tor节点；
   Onionite (https://github.com/lukechilds/onionite) - 有关节点的信息；
   Tor Metrics (https://metrics.torproject.org/) - 有关节点的信息；

1. 爬虫
   TorBot (https://github.com/DedSecInside/TorBot) - 用 Python 编写的智能开源情报工具；

   OnionBot (https://github.com/Flobin/OnionBot) - 以twitter机器人形式实现的 .onion网站爬虫；
   OnionIngestor (https://github.com/danieleperera/OnionIngestor) - 用于收集.onion 网站信息并将其编入 Elasticsearch 索引的工具；
   Midnight Sea (https://github.com/RicYaben/midnight_sea) - 模拟人类行为的暗网市场通用爬虫；
   VililantOnion (https://github.com/andreyglauzer/VigilantOnion) - 关键字搜索爬虫；
   OnionScan (https://github.com/s-rah/onionscan) - 另一款不错的洋葱网站爬虫。
   Darkweb Crawler Project (https://github.com/JarryShaw/darc)- 一个古老/经典的但仍可用的爬虫。依旧有更新；
   Fresh Onions TOR Hidden Service Crawler (https://

github.com/dirtyfilthy/freshonions-torscraper) - 另一个老式爬网程序，可将站点收集到 Fresh Onions 目录中。

1. Tor搜索引擎（脚本）
Katana (https://github.com/TebbaaX/Katana) - 自动执行dorking并支持Tor的工具，python脚本；
OnionSearch (https://github.com/megadose/OnionSearch) - 另一个python脚本，用于收集Tor中不同搜索引擎的链接；
Darkdump (https://github.com/josh0xA/darkdump) - 直接从您的终端搜索深网；
Darkus (https://github.com/Lucksi/Darkus) - 洋葱网站关键词搜索引擎。

1. Tor 中的搜索引擎（网站）
EXCAVATOR
http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5f
Devil Search http://
search65pq2x5oh4o4qlxk2zvoa5zhbfi6mx4br4oc33rpxuayauwsqd.on
Ahima (clear) https://ahmia.fi/
TorDex http://
tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onio
Torgle http://
iy3544gmoeclh5de6gez2256v6pjh4omhpqdh2wpeeppjtvqmjhkfwad.o
torgle/
Raklet http://
iwr4usy33opfclmbyemzbmnwwnmmqpqltezpac7fyqqkdv3mabtm6kq
Phobos http://
phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion
Onion Search Engine (clear) http://
kn3hl4xwon63tc6hpjrwza2npb7d4w5yhbzq7jjewpfzyhsd65tm6dad.o

.onion 目录精选

1. UnderDir http://
underdiriled6lvdfgiw4e5urfofuslnz7ewictzf76h4qb73fxbsxad.onion/

1. Hidden Links http://wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion

1. Dark Eye http://darkeyepxw7cuu2cppnjlgqaav6j42gyt43clcn4vjjf7llfyly5cxid.onion/

1. Fresh Onions http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad

1. Signpost http://signpostcjbbviqdhfbtocj6dthbd7cpvo3tpwrrfhkkk4fafjd53nyd.onion/

1. Deep Link http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.onio

1. Deep Links Dump http://deepqelxz6iddqi5obzla2bbwh5ssyqqobxin27uzkr624wtubhto3ad.onio

1. dark.fail https://dark.fail/

1. Tasty Onions http://22tojepqmpah32fkeuurutki7o5bmb45uhmgzdg4l2tk34fkdafgt

1. tor.taxi https://tor.taxi/

1. Dark Catalog http://catalogxlotjjnu6vyevngf675vu6beefzxw6gd6a3fwgmgznksrqmqd.onio latest.html

1. Onion link list http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/

1. Onion link online test http://

donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/test.php

1. Deep Link Onion Directory http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.oni

1. Dark Web Pug's Ultimate Guide http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.oni

1. TOR Links List http://5n4qdkw2wavc55peppyrelmb2rgsx7ohcb2tkxhub2gyfurxulfyd

1. Hidden Wiki FRESH 2022 http://ieeppzy7cz254nz2iz7omykshnlap5ktjq3r7ujfpxagygaobpxfdbqd.onion

[image]
[image]

Tor工具系列

[image] 关键词	tor 反封锁 安全搜索 暗网
[image] 关联	[image]完全Tor
[image] 创建时间	2023年11月6日
[image] Description	工具

1. TOR Node List (https://www.dan.me.uk/tornodes) - 节点列表；

1. Onionite (https://github.com/lukechilds/onionite) - 有关节点的信息；

1. Tor Metrics (https://metrics.torproject.org/) - 节点信息；

1. TorBot (https://github.com/DedSecInside/TorBot) 是一款用Python编写的智能开源情报工具。

1. OnionBot (https://github.com/Flobin/OnionBot) 是一款以twitter机器人形式实现的.onion网站爬虫。

1. OnionScan (https://github.com/s-rah/onionscan) - 另一款优秀的洋葱网站爬虫。

1. VililantOnion (https://github.com/andreyglauzer/VigilantOnion) - 通过关键字进行搜索的爬虫。

1. OnionIngestor (https://github.com/danieleperera/OnionIngestor) - 用于收集和抓取.onion 网站并将收集到的信息编入 Elasticsearch 索引的工具。

1. Darkus (https://github.com/Lucksi/Darkus) 是一款使用关键字的洋葱网站搜索引擎。

暗网开源情报Full Pack

1. 网络信息
TOR Node List (https://www.dan.me.uk/tornodes) - 节点列表；
ExoneraTor (https://metrics.torproject.org/exonerator.html) - 检查IP是否用作Tor节点；
Onionite (https://github.com/lukechilds/onionite) - 有关节点的信息；
Tor Metrics (https://metrics.torproject.org/) - 有关节点的信息；

1. 爬虫
TorBot (https://github.com/DedSecInside/TorBot) - 用 Python 编写的智能开源情报工具；

OnionBot (https://github.com/Flobin/OnionBot) - 以twitter机器人形式实现的 .onion网站爬虫；
OnionIngestor (https://github.com/danieleperera/OnionIngestor) - 用于收集.onion 网站信息并将其编入 Elasticsearch 索引的工具；
Midnight Sea (https://github.com/RicYaben/midnight_sea) - 模拟人类行为的暗网市场通用爬虫；
VililantOnion (https://github.com/andreyglauzer/VigilantOnion) - 关键字搜索爬虫；
OnionScan (https://github.com/s-rah/onionscan) - 另一款不错的洋葱网站爬虫。
Darkweb Crawler Project (https://github.com/JarryShaw/

darc)- 一个古老/经典的但仍可用的爬虫。依旧有更新；
Fresh Onions TOR Hidden Service Crawler (https://github.com/dirtyfilthy/freshonions-torscraper) - 另一个老式爬网程序，可将站点收集到 Fresh Onions 目录中。

1. Tor搜索引擎（脚本）
   Katana (https://github.com/TebbaaX/Katana) - 自动执行dorking并支持Tor的工具，python脚本；
   OnionSearch (https://github.com/megadose/OnionSearch) - 另一个python脚本，用于收集Tor中不同搜索引擎的链接；
   Darkdump (https://github.com/josh0xA/darkdump) - 直接从您的终端搜索深网；
   Darkus (https://github.com/Lucksi/Darkus) - 洋葱网站关键词搜索引擎。

1. Tor 中的搜索引擎（网站）
   EXCAVATOR
   http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5f
   Devil Search http://search65pq2x5oh4o4qlxk2zvoa5zhbfi6mx4br4oc33rpxuayauwsqd.on
   Ahima (clear) https://ahmia.fi/
   TorDex http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onic
   Torgle http://iy3544gmoeclh5de6gez2256v6pjh4omhpqdh2wpeeppjtvqmjhkfwad.c
   torgle/
   Raklet http://iwr4usy33opfclmbyemzbmnwwnmmqpqltezpac7fyqqkdv3mabtm6kq
   Phobos http://phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion
   Onion Search Engine (clear) http://kn3hl4xwon63tc6hpjrwza2npb7d4w5yhbzq7jjewpfzyhsd65tm6dad.o

.onion 目录精选

1. UnderDir http://

underdiriled6lvdfgiw4e5urfofuslnz7ewictzf76h4qb73fxbsxad.onion/

1. Hidden Links http://wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion

1. Dark Eye http://darkeyepxw7cuu2cppnjlgqaav6j42gyt43clcn4vjjf7llfyly5cxid.onion/

1. Fresh Onions http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad

1. Signpost http://signpostcjbbviqdhfbtocj6dthbd7cpvo3tpwrrfhkkk4fafjd53nyd.onion/

1. Deep Link http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.onio

1. Deep Links Dump http://deepqelxz6iddqi5obzla2bbwh5ssyqqobxin27uzkr624wtubhto3ad.onio

1. dark.fail https://dark.fail/

1. Tasty Onions http://22tojepqmpah32fkeuurutki7o5bmb45uhmgzdg4l2tk34fkdafgt

1. tor.taxi https://tor.taxi/

1. Dark Catalog http://catalogxlotjjnu6vyevngf675vu6beefzxw6gd6a3fwgmgznksrqmqd.onio latest.html

1. Onion link list http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/

1. Onion link online test http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/test.php

1. Deep Link Onion Directory http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.oni

1. Dark Web Pug's Ultimate Guide http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.oni

1. TOR Links List http://5n4qdkw2wavc55peppyrelmb2rgsx7ohcb2tkxhub2gyfurxulfyd

1. Hidden Wiki FRESH 2022 http://ieeppzy7cz254nz2iz7omykshnlap5ktjq3r7ujfpxagygaobpxfdbqd.onion

[image]
[image]

访问网站时保护自己的敏感数据

[image] 关键词	URL 免追踪 自助
[image] 创建时间	2023/11/09
[image] **Description**	工具

如果您不想每次访问网站时都花时间阅读用户协议，可以使用 ToSDR 服务。这项服务可以帮助您在访问网站资源时保护自己的敏感数据。

该服务会对网站进行评估，并给出一个评级，帮助您了解隐私风险有多大。评级 "F"表示隐私非常糟糕，"A"表示非常好。此外，该服务还有一个扩展功能，使用起来可以更方便。

 https://tosdr.org/

[image]
[image]

访问网站时保护自己的敏感数据

[image] 关键词	URL 免追踪 自助
[image] 创建时间	2023年11月9日
[image] **Description**	工具

如果您不想每次访问网站时都花时间阅读用户协议，可以使用 ToSDR 服务。这项服务可以帮助您在访问网站资源时保护自己的敏感数据。

该服务会对网站进行评估，并给出一个评级，帮助您了解隐私风险有多大。评级 "F"表示隐私非常糟糕，"A"表示非常好。此外，该服务还有一个扩展功能，使用起来可以更方便。

 https://tosdr.org/

[image]
[image]

基于云的多用户 Chrome 浏览器

[image] 关键词		团队 效率
[image] 创建时间		2023年11月13日
[image] **Description**		工具

Remote Browser Embed - 这是一个基于云的多用户 Chrome 浏览器，您可以将其嵌入到您的项目中。

只需点击一下，就可以让用户开始实时协作编辑和浏览网页，或在屏幕上添加注释，以阐明想法或指导同事。

该服务适用于虚拟办公室、会议室、销售或培训工作。

 https://www.producthunt.com/products/remote-browser-embed

[image]
[image]

基于云的多用户 Chrome 浏览器

[image]	关键词	团队 效率
[image]	创建时间	2023/11/13
[image]	**Description**	工具

Remote Browser Embed - 这是一个基于云的多用户 Chrome 浏览器，您可以将其嵌入到您的项目中。

只需点击一下，就可以让用户开始实时协作编辑和浏览网页，或在屏幕上添加注释，以阐明想法或指导同事。

该服务适用于虚拟办公室、会议室、销售或培训工作。

 https://www.producthunt.com/products/remote-browser-embed

[image]
[image]

绕开面部识别

[image] 关键词	免追踪 防御 预防性
[image] 创建时间	2023/11/29
[image] **Description**	工具

自动绕过面部识别，躲避窥探。

Anonymous Camera 是一款在拍摄过程中自动在照片视频中隐藏面部的应用程序。您还可以隐藏整个身体或部分身体，如：衣服、纹身、疤痕、头发等。

隐藏有多种类型，包括常见的 "模糊"开始，也可以在脸部区域覆盖一个单一颜色的圆圈。

其他功能还包括变声、隐藏元数据，都在本地进行，没有云风险。

目前只在 App Store 上提供。是免费的，但附加功能可以以 1.99 美元的价格购买。

 https://apps.apple.com/us/app/anonymous-camera/id1504102584

[image]
[image]

绕开面部识别

[image] 关键词	免追踪 防御 预防性
[image] 创建时间	2023年11月29日
[image] **Description**	工具

自动绕过面部识别，躲避窥探。

Anonymous Camera 是一款在拍摄过程中自动在照片视频中隐藏面部的应用程序。您还可以隐藏整个身体或部分身体，如：衣服、纹身、疤痕、头发等。

隐藏有多种类型，包括常见的 "模糊"开始，也可以在脸部区域覆盖一个单一颜色的圆圈。

其他功能还包括变声、隐藏元数据，都在本地进行，没有云风险。

目前只在 App Store 上提供。是免费的，但附加功能可以以 1.99 美元的价格购买。

 https://apps.apple.com/us/app/anonymous-camera/id1504102584

[image]
[image]

一些注重隐私的浏览器扩展

[image] 关键词	数字足迹 电脑 预防性
[image] 创建时间	2023年12月6日
[image] **Description**	工具

1、Self Destructing Cookies (https://add0n.com/self-destructing-cookies.html) - 在您离开网站后立即删除 Cookie。

2、WebRTC Leak Prevent (https://github.com/aghorler/WebRTC-Leak-Prevent) - 允许您在Chromium浏览器中禁用WebRTC。在 Firefox 中则在设置中禁用。

3、ScriptSafe (https://github.com/andryou/scriptsafe) - 可以阻止某些脚本的执行。

4、Site Bleacher (https://github.com/wooque/site-bleacher) - 自动删除 cookie、本地存储、IndexedDB 和Service Worker。

5、Skip Redirect (https://github.com/sblask/webextension-skip-redirect) - 跳过链接中嵌入的所有重定向站点，直接指向最终站点。

6、Web Archives (https://github.com/dessant/web-archives/wiki/Search-engines) - 允许您从多种存档和缓存源中进行搜索，允许您：Wayback Machine、Archive is、Google 和其他。

[image]
[image]

一些注重隐私的浏览器扩展

[image] 关键词	数字足迹 电脑 预防性
[image] 创建时间	2023/12/06
[image] **Description**	工具

1、Self Destructing Cookies (https://add0n.com/self-destructing-cookies.html) - 在您离开网站后立即删除 Cookie。

2、WebRTC Leak Prevent (https://github.com/aghorler/WebRTC-Leak-Prevent) - 允许您在Chromium浏览器中禁用WebRTC。在 Firefox 中则在设置中禁用。

3、ScriptSafe (https://github.com/andryou/scriptsafe) - 可以阻止某些脚本的执行。

4、Site Bleacher (https://github.com/wooque/site-bleacher) - 自动删除 cookie、本地存储、IndexedDB 和Service Worker。

5、Skip Redirect (https://github.com/sblask/webextension-skip-redirect) - 跳过链接中嵌入的所有重定向站点，直接指向最终站点。

6、Web Archives (https://github.com/dessant/web-archives/wiki/Search-engines) - 允许您从多种存档和缓存源中进行搜索，允许您：Wayback Machine、Archive is、Google 和其他。

[image]
[image]

一些可选的翻译服务

[image] 关键词	个人 团队 效率
[image] 创建时间	2023/12/08
[image] **Description**	工具

1. DeepL Translate (https://www.deepl.com/translator) 是一款基于机器翻译的在线翻译软件。可翻译整个文件中的文本。免费版本有限制。对于 Android 用户，F-Droid 中有一个非官方的应用。

1. SimplyTranslate (https://simplytranslate.org/) 是多个翻译器的替代前端，注重隐私。包括 Google、LibreTranslate、ICIBA、Reverso 等。

1. Stepes (https://www.stepes.com/ai-powered-translation-managment-system/) 不仅能翻译文本，还能一次性翻译整个文件，有两种翻译选项：人工智能驱动和自动翻译。

1. Reverso Context (https://context.reverso.net/翻译/) - 在线翻译，具有同义词搜索和上下文翻译搜索功能。

1. LanguageTool (https://languagetool.org/?force_language=1) - Grammarly 的替代软件。可检查文本中的语法和标点符号。

1. SimplyTranslate Mobile (https://f-droid.org/packages/com.simplytranslate_mobile/) - 另一款谷歌前端，不过是一款安卓应用。有通过摄像头识别文字的功能，支持 108 种语言。

1. PDNob Image Translator (https://www.pdnob.com/) - 一键捕捉、识别并翻译图片和 PDF 中的文字。

1. LibreTranslate (https://libretranslate.com/?source=auto&target=en&q=) - 另一款基于机器翻译的翻译器。100% 独立项目。

1. Taia (https://taia.io/) - 不错的人工智能翻译器，免费但需要注册。支持 97 种语言。

1. Paraphrase Tool (https://paraphrasetool.com/) - 用 100 种语言转述您的文本。

1. Firefox Translations (https://addons.mozilla.org/en-GB/firefox/addon/firefox-translations/?utm_source=addons.mozilla.org&utm_medium=referral&utm_conten - 将整个页面翻译成您想要的语言。

1. Machine Translation (https://www.machinetranslation.com/) - 机器智能翻译器。使用不同的翻译器：DeepL、谷歌、亚马逊等。

[image]
[image]

一些可选的翻译服务

[image] 关键词	个人 团队 效率
[image] 关联	[image]翻译视频 ；[image]实时语音翻译 ；[image]实时语音翻译 ；[image]一系列免费的人工智能翻译器 ；[image]跨平台AI翻译
[image] 创建时间	2023年12月8日
[image] **Description**	工具

1. DeepL Translate (https://www.deepl.com/translator) 是一款基于机器翻译的在线翻译软件。可翻译整个文件中的文本。免费版本有限制。对于 Android 用户，F-Droid 中有一个非官方的应用。

1. SimplyTranslate (https://simplytranslate.org/) 是多个翻译器的替代前端，注重隐私。包括 Google、LibreTranslate、ICIBA、Reverso 等。

1. Stepes (https://www.stepes.com/ai-powered-translation-managment-system/) 不仅能翻译文本，还能一次性翻译整个文件，有两种翻译选项：人工智能驱动和自动翻译。

1. Reverso Context (https://context.reverso.net/翻译/) - 在线翻译，具有同义词搜索和上下文翻译搜索功能。

1. LanguageTool (https://languagetool.org/?force_language=1) - Grammarly 的替代软件。可检查文本中的语法和标点符号。

1. SimplyTranslate Mobile (https://f-droid.org/packages/com.simplytranslate_mobile/) - 另一款谷歌前端，不过是一款安卓应用。有通过摄像头识别文字的功能，支持 108 种语言。

1. PDNob Image Translator (https://www.pdnob.com/) - 一键捕捉、识别并翻译图片和 PDF 中的文字。

1. LibreTranslate (https://libretranslate.com/?source=auto&target=en&q=) - 另一款基于机器翻译的翻译器。100% 独立项目。

1. Taia (https://taia.io/) - 不错的人工智能翻译器，免费但需要注册。支持 97 种语言。

1. Paraphrase Tool (https://paraphrasetool.com/) - 用 100 种语言转述您的文本。

1. Firefox Translations (https://addons.mozilla.org/en-GB/firefox/addon/firefox-translations/?utm_source=addons.mozilla.org&utm_medium=referral&utm_conten
- 将整个页面翻译成您想要的语言。

1. Machine Translation (https://www.machinetranslation.com/) - 机器智能翻译器。使用不同的翻译器：DeepL、谷歌、亚马逊等。

[image]
[image]

隐私自助：流行产品的开源替代品目录

[image] 关键词	免追踪 反侦察 安全搜索 数字足迹
[image] 创建时间	2023/12/14
[image] **Description**	工具

Osssoftware 是流行产品的开源替代品目录。

该目录相对较新，并在不断补充中。目前您可以在其中找到300多种开源产品。

也许您知道同类的 Alternative To，但到目前为止，它的规模相比下要小得多。

对于安卓用户，可推荐替代应用商店：Aurora Store 和 F-Droid。

 https://osssoftware.org/open-source-alternatives/

[image]
[image]

隐私自助：流行产品的开源替代品目录

[image] 关键词	免追踪 反侦察 安全搜索 数字足迹
[image] 关联	[image]监视资本主义之外的元搜索引擎
[image] 创建时间	2023年12月14日
[image] **Description**	工具

Osssoftware 是流行产品的开源替代品目录。

该目录相对较新，并在不断补充中。目前您可以在其中找到300多种开源产品。

也许您知道同类的 Alternative To，但到目前为止，它的规模相比下要小得多。

对于安卓用户，可推荐替代应用商店：Aurora Store 和 F-Droid。

 https://osssoftware.org/open-source-alternatives/

[image]
[image]

一系列隐写工具

[image] 关键词	传输安全 加密 隐写术
[image] 创建时间	2023年12月19日
[image] **Description**	工具

第 1 部分（Windows工具）

1、DeepSound (https://github.com/Jpinsoft/DeepSound) - 可以将数据隐藏在音频文件中。可以嵌入任何类型的文件，并根据容器大小和音频质量设置自动计算可用空间。

2、Hallucinate (https://sourceforge.net/projects/hallucinate/) - 这款小巧的工具（仅34Kb）用Java编写，无需安装。作为容器，它支持BMP和PNG格式，比Anubis方便得多。

3、 JHide (https://sourceforge.net/projects/jhideapp/) - 另一款小巧的工具，与 Hallucinate 不同的是，除了支持 BMP和 PNG格式外，还支持TIFF格式，而且还允许使用密码保护。

4、 OpenPuff（ https://embeddedsw.net/OpenPuff_download.html ）- 最新版本（4.00）不仅支持将某些文件隐藏在其他文件中，还支持处理任意格式的隐写。还可以通过添加水印来证明您是合法所有者。与其他同类工具的不同之处在于，OpenPuff可以使用功能强大的伪随机数生成器进行加密。

5、OpenStego (https://www.openstego.com/) - 该程序可在

Windows和Linux上运行。它支持BMP、PNG、JPG、GIF和WBMP。填充的容器总是以PNG格式保存。

第 2 部分

1、Cloakify (https://github.com/TryCatchHCF/Cloakify) - 文本隐写工具，易于扩展。特点是在隐写前进行 Base64编码。

2、Steghide (https://github.com/StefanoDeVuono/steghide) - C++ 编写的控制台程序。可将信息隐藏在各种图像和音频文件中。支持JPEG、BMP、WAV和AU格式。

3、Spectrology (https://github.com/solusipse/spectrology) - 可在声音文件中隐藏秘密图片的工具。可以选择要使用的频率范围，支持所有流行的图像编解码器。

4、ImageSpyer G2 (https://freesoft.net/windows/imagespyer_g2) - 可在图片中隐藏秘密文件，同时数据将得到两层加密保护。这是一个没有官方网站的老程序。

5、 OpenStego (https://github.com/syvaidya/openstego/releases) - 该软件用Java实现，支持AES加密，在想要了解隐写术的用户中很受欢迎。支持插件，因此您可以自己实现某种隐写算法。有 Windows 和 Linux 版本。

6、 SilentEye (https://achorein.github.io/silenteye/) - 是一款界面简单的跨平台软件。它拥有很多插件和一个漂亮的图形用户界面。使用新的隐写算法和加密。

[image]
[image]

一系列隐写工具

[image] 关键词	传输安全 加密 隐写术
[image] 创建时间	2023/12/19
[image] **Description**	工具

第 1 部分（**Windows**工具）

1、DeepSound (https://github.com/Jpinsoft/DeepSound) - 可以将数据隐藏在音频文件中。可以嵌入任何类型的文件，并根据容器大小和音频质量设置自动计算可用空间。

2、Hallucinate (https://sourceforge.net/projects/hallucinate/) - 这款小巧的工具（仅34Kb）用Java编写，无需安装。作为容器，它支持BMP和PNG格式，比Anubis方便得多。

3、 JHide (https://sourceforge.net/projects/jhideapp/) - 另一款小巧的工具，与 Hallucinate 不同的是，除了支持 BMP和 PNG格式外，还支持TIFF格式，而且还允许使用密码保护。

4、 OpenPuff（ https://embeddedsw.net/OpenPuff_download.html ）- 最新版本（4.00）不仅支持将某些文件隐藏在其他文件中，还支持处理任意格式的隐写。还可以通过添加水印来证明您是合法所有者。与其他同类工具的不同之处在于，OpenPuff可以使用功能强大的伪随机数生成器进行加密。

5、OpenStego (https://www.openstego.com/) - 该程序可在

Windows和Linux上运行。它支持BMP、PNG、JPG、GIF和WBMP。填充的容器总是以PNG格式保存。

第 2 部分

1、Cloakify (https://github.com/TryCatchHCF/Cloakify) - 文本隐写工具，易于扩展。特点是在隐写前进行 Base64编码。

2、Steghide (https://github.com/StefanoDeVuono/steghide) - C++ 编写的控制台程序。可将信息隐藏在各种图像和音频文件中。支持JPEG、BMP、WAV和AU格式。

3、Spectrology (https://github.com/solusipse/spectrology) - 可在声音文件中隐藏秘密图片的工具。可以选择要使用的频率范围，支持所有流行的图像编解码器。

4、ImageSpyer G2 (https://freesoft.net/windows/imagespyer_g2) - 可在图片中隐藏秘密文件，同时数据将得到两层加密保护。这是一个没有官方网站的老程序。

5、 OpenStego (https://github.com/syvaidya/openstego/releases) - 该软件用Java实现，支持AES加密，在想要了解隐写术的用户中很受欢迎。支持插件，因此您可以自己实现某种隐写算法。有 Windows 和 Linux 版本。

6、 SilentEye (https://achorein.github.io/silenteye/) - 是一款界面简单的跨平台软件。它拥有很多插件和一个漂亮的图形用户界面。使用新的隐写算法和加密。

[image]
[image]

浏览器中的流媒体工作室

[image] 关键词		效率
[image] 创建时间		2023年12月23日
[image] **Description**		工具

StreamYard 是浏览器中的流媒体工作室。

该工具可让您轻松地在多个平台上同时向所有受众直播您的节目。采访嘉宾、同步评论等等。

此外，冗余服务器可确保您的直播无论如何都不会中断。

直接向 Facebook、YouTube、LinkedIn 和其他平台创建专业直播的最简单方法。

 https://streamyard.com/

[image]
[image]

浏览器中的流媒体工作室

[image] 关键词	效率
[image] 创建时间	2023/12/23
[image] **Description**	工具

StreamYard 是浏览器中的流媒体工作室。

该工具可让您轻松地在多个平台上同时向所有受众直播您的节目。采访嘉宾、同步评论等等。

此外，冗余服务器可确保您的直播无论如何都不会中断。

直接向 Facebook、YouTube、LinkedIn 和其他平台创建专业直播的最简单方法。

 https://streamyard.com/

[image]
[image]

安全地存储秘密

[image] 关键词	QR码 传输安全 加密
[image] 创建时间	2024年1月12日
[image] Description	工具

Hyperbacked 使用包含加密QR码的可打印 PDF 文件安全地存储秘密。

加密备份可进一步分段，以便分发给许多受信任方。

特点包括自由开源、秘密共享、合理推诿、256位AES-GCM加密，可在Windows、macOS 和 GNU/Linux 上使用。

 https://github.com/Twometer/hyperbacked

[image]
[image]

安全地存储秘密

[image] 关键词	QR码 传输安全 加密
[image] 创建时间	2024/01/12
[image] **Description**	工具

Hyperbacked 使用包含加密QR码的可打印 PDF 文件安全地存储秘密。

加密备份可进一步分段，以便分发给许多受信任方。

特点包括自由开源、秘密共享、合理推诿、256位AES-GCM加密，可在Windows、macOS 和 GNU/Linux 上使用。

 https://github.com/Twometer/hyperbacked

[image]
[image]

为孤军奋战者准备的预警方案

[image] 关键词	反间谍 强迫失踪 报警 独居 自助防御 预防性
[image] 关联	[image]自托管黑头套紧急响应 ；预防‘黑头套’ ；为孤军奋战者准备的预警方案 ；藏匿点或安全屋 ；**S01E01-T2** 识别威胁并作出反应 ；抢先采取行动 **-** 反侦基础课 **S06E01**：七点规则和态势感知 ；
[image] 创建时间	2024年1月17日
[image] **Description**	工具

Keep Alive 是一款应用程序，可在一段时间内未使用设备时通过SMS发送预定的特殊信息。

该应用的设计目的是在发生事故或紧急情况时保护孤独的人。比如孤军奋战的敏感人士/匿名工作者，一旦遭遇绑架/强迫失踪（黑头套），可快速求救。

该应用使用设备的锁屏来检测活动，如果没有活动，就会显示 "你在吗？" 的提示。

如果通知未得到确认，该程序就会激活警报，并发送短信或致电您预定的紧急联系人。

该程序还可以在短信中包含位置信息，并拨打免提电话。

它不使用云服务，不需要账户，免费、无广告、无跟踪器。

□ https://github.com/keepalivedev/KeepAlive

[image]
[image]

为孤军奋战者准备的预警方案

[image] 关键词	反间谍 强迫失踪 报警 独居 自助 防御 预防性
[image] 创建时间	2024/01/17
[image] **Description**	工具

Keep Alive 是一款应用程序，可在一段时间内未使用设备时通过SMS发送预定的特殊信息。

该应用的设计目的是在发生事故或紧急情况时保护孤独的人。比如孤军奋战的敏感人士/匿名工作者，一旦遭遇绑架/强迫失踪（黑头套），可快速求救。

该应用使用设备的锁屏来检测活动，如果没有活动，就会显示 "你在吗？" 的提示。

如果通知未得到确认，该程序就会激活警报，并发送短信或致电您预定的紧急联系人。

该程序还可以在短信中包含位置信息，并拨打免提电话。

它不使用云服务，不需要账户，免费、无广告、无跟踪器。

□ https://github.com/keepalivedev/KeepAlive

[image]
[image]

打破付费墙

[image]	关键词	付费墙 信息民主化
[image]	创建时间	2024/01/29
[image]	**Description**	工具

知识应该共享而不是商品化。信息自由是民主和明智决策的重要支柱。

Ladder 是一种网络代理服务器，可帮您绕开 付费墙。

它旨在平衡媒体机构的经济利益与公众获取信息的权利。

Ladder 的功能包括绕过付费访问、移除CORS标头、应用基于域的规则以及保持网站可访问。

它还有API，支持自定义用户代理，并有一个Docker容器。

Ladder 可移除大部分广告，支持基本认证，禁用日志记录，并且无追踪。
有可选的TOR代理。
如果内容不可用，Ladder可以从谷歌缓存中检索信息。

局限性包括某些网站的格式问题，以及无法访问不向搜索引擎提供内容的网站的内容。

一定程度上还可用于规避封锁。

https://github.com/kubero-dev/ladder

[image]
[image]

打破付费墙

[image]	关键词	付费墙 信息民主化
[image]	创建时间	2024年1月29日
[image]	**Description**	工具

知识应该共享而不是商品化。信息自由是民主和明智决策的重要支柱。

Ladder 是一种网络代理服务器，可帮您绕开 付费墙。

它旨在平衡媒体机构的经济利益与公众获取信息的权利。

Ladder 的功能包括绕过付费访问、移除CORS标头、应用基于域的规则以及保持网站可访问。

它还有API，支持自定义用户代理，并有一个Docker容器。

Ladder 可移除大部分广告，支持基本认证，禁用日志记录，并且无追踪。
有可选的TOR代理。
如果内容不可用，Ladder可以从谷歌缓存中检索信息。

局限性包括某些网站的格式问题，以及无法访问不向搜索引擎提供内容的网站的内容。

一定程度上还可用于规避封锁。

□ https://github.com/kubero-dev/ladder

[image]
[image]

在坏人强行访问您的设备的情况下抹除数据

[image] 关键词	反侦察 移动设备 自助 预防性
[image] 创建时间	2024年3月6日
[image] **Description**	工具

紧急按钮的概念是为了在极端情况下擦除敏感数据（例如设备被警察抢走或丢失时）。本帖将描述的是为此目的的Android手机的设置方式。

首先是创建一个所谓的"工作配置文件"，它最初的目的是将工作应用程序与个人应用程序隔离开。在创建加密容器或第二系统之前，这种方法的优点是速度快，不需要root权限、自定义恢复等。这里的目的是要创造出“本来就没有数据”的样子，而不是坚硬的防攻击性能。

~ 首先，安装 Shelter（https://f-droid.org/packages/net.typeblog.shelter/ ）；
~ 通过 Shelter 将敏感应用程序和数据安装或克隆到工作配置文件中，从主配置文件中删除它们；
~ 将Wasted (https://github.com/x13a/Wasted) 放入工作配置文件（将接受来自Duress的信号）；
~ 在主配置文件中设置Duress (https://github.com/x13a/Duress)（将发出删除信号）。

📌 Wasted：

1. 复制颜色窗口中的代码；

1. 勾选 "擦除数据"；

1. 将屏幕底部的按钮从 "O"切换到 "I"（打开）；

1. 申请设备管理权限 - 需要这样才能执行清除；

1. 在设置中勾选 "广播信息" - 将接受来自Duress的信号。

📌 Duress：

1. 在 "action"中输入 me.lucky.wasted.action.TRIGGER；

1. receiver：me.lucky.wasted/TriggerReceiver；

1. key: code；

1. value: 从Wasted复制的那个代码；

1. PIN：向Wasted发送信号的解锁密码；

1. Keyguard: A；

1. 底部按钮：位置 "I"。

完成。现在，当您输入Duress设置步骤5中选择的解锁密码时，工作配置文件中的所有内容都将被清除。

您还可以构想其他可能的组合场景，以满足特定需求。

[image]

返回：[image]如果您的手机被盗或被警察抢走...

返回：[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？

返回：[image]如何保持 Android 设备免受警察的侵害

[image]
[image]

在坏人强行访问您的设备的情况下抹除数据

[image] 关键词	反侦察 移动设备 自助 预防性
[image] 创建时间	2024/03/06
[image] **Description**	工具

紧急按钮的概念是为了在极端情况下擦除敏感数据（例如设备被警察抢走或丢失时）。本帖将描述的是为此目的的Android手机的设置方式。

首先是创建一个所谓的"工作配置文件"，它最初的目的是将工作应用程序与个人应用程序隔离开。在创建加密容器或第二系统之前，这种方法的优点是速度快，不需要root权限、自定义恢复等。这里的目的是要创造出“本来就没有数据”的样子，而不是坚硬的防攻击性能。

~ 首先，安装 Shelter（https://f-droid.org/packages/net.typeblog.shelter/ ）；
~ 通过 Shelter 将敏感应用程序和数据安装或克隆到工作配置文件中，从主配置文件中删除它们；
~ 将Wasted (https://github.com/x13a/Wasted) 放入工作配置文件（将接受来自Duress的信号）；
~ 在主配置文件中设置Duress (https://github.com/x13a/Duress)（将发出删除信号）。

📌 Wasted：

1. 复制颜色窗口中的代码；

1. 勾选 "擦除数据"；

1. 将屏幕底部的按钮从 "O"切换到 "I"（打开）；

1. 申请设备管理权限 - 需要这样才能执行清除；

1. 在设置中勾选 "广播信息" - 将接受来自Duress的信号。

📌 Duress：

1. 在 "action"中输入 me.lucky.wasted.action.TRIGGER；

1. receiver：me.lucky.wasted/TriggerReceiver；

1. key: code；

1. value: 从Wasted复制的那个代码；

1. PIN：向Wasted发送信号的解锁密码；

1. Keyguard: A；

1. 底部按钮：位置 "I"。

完成。现在，当您输入Duress设置步骤5中选择的解锁密码时，工作配置文件中的所有内容都将被清除。

您还可以构想其他可能的组合场景，以满足特定需求。

如果您错过了：

- 《如果您的手机被盗或被警察抢走...》
- 《如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？》
- 《如何让您的 iPhone 能够防小偷》
- 《如何保持 Android 设备免受警察的侵害》

[image]
[image]

免费读书

[image]	关键词	信息民主化 海盗
[image]	关联	[image]一系列免费的人工智能翻译器 ；[image]一些可选的翻译服务 ；
[image]	创建时间	2024年3月11日
[image]	**Description**	工具

Openlib 是一款开源 Android 应用程序，用于从海盗影子图书馆（Anna's Archive）下载和阅读图书。

Openlib 的部分功能包括趋势、内置图书阅读器、支持 epub 和 pdf 格式、在您喜爱的电子书阅读器中打开图书、对图书进行过滤和排序。

由于 Anna's Archive 没有API，该应用程序的工作方式是向其发送请求并分析响应。
然后从响应中提取镜像并下载图书。

 https://github.com/dstark5/Openlib

 IzzyOnDroid: https://android.izzysoft.de/repo/apk/com.app.openlib

[image]
[image]

免费读书

[image]	关键词	信息民主化 海盗
[image]	创建时间	2024/03/11
[image]	**Description**	工具

Openlib 是一款开源 Android 应用程序，用于从海盗影子图书馆（Anna's Archive）下载和阅读图书。

Openlib 的部分功能包括趋势、内置图书阅读器、支持 epub 和 pdf 格式、在您喜爱的电子书阅读器中打开图书、对图书进行过滤和排序。

由于 Anna's Archive 没有API，该应用程序的工作方式是向其发送请求并分析响应。
然后从响应中提取镜像并下载图书。

 https://github.com/dstark5/Openlib

 IzzyOnDroid: https://android.izzysoft.de/repo/apk/com.app.openlib

[image]
[image]

端对端加密笔记

[image] 关键词	P2P 加密
[image] 创建时间	2024年3月14日
[image] **Description**	工具

Standard Notes 是一款具有端到端加密功能的笔记应用。

它提供快速、免费和加密的跨平台同步功能，可跨越不限数量的设备。

用户可以使用开源代码实现自托管。

该应用程序适用于 Mac、Windows、GNU/Linux、iOS 和 Android。

 https://github.com/standardnotes/app

 F-droid: https://f-droid.org/ru/packages/com.standardnotes/

 网站：https://standardnotes.com/

[image]
[image]

端对端加密笔记

[image] 关键词		P2P 加密
[image] 创建时间		2024/03/14
[image] **Description**		工具

Standard Notes 是一款具有端到端加密功能的笔记应用。

它提供快速、免费和加密的跨平台同步功能，可跨越不限数量的设备。

用户可以使用开源代码实现自托管。

该应用程序适用于 Mac、Windows、GNU/Linux、iOS 和 Android。

 https://github.com/standardnotes/app

 F-droid: https://f-droid.org/ru/packages/com.standardnotes/

 网站：https://standardnotes.com/

[image]
[image]

安卓文件管理器

[image] 关键词 安卓 查询整理

[image] 创建时间 2024/03/18

[image] **Description** 工具

Little File Explorer 是一款适用于安卓的小巧简单的文件管理器，在设计时充分考虑了兼容性。

▫免费
▫足够小 (＜ 40KB)
▫满足基本文件操作（剪切、复制、粘贴、重命名、删除）
▫文件名过滤器
▫按名称和修改时间排序
▫ 在SD卡和内部存储之间轻松切换
▫文件/文件夹路径复制
▫最低权限
▫ 暗模式
▫□ MD5校验和生成与验证

□ https://github.com/martinmimigames/little-file-explorer

□ F-Droid: https://f-droid.org/ru/packages/com.martinmimigames.simplefileexplorer/

[image]
[image]

安卓文件管理器

[image]	关键词	安卓 查询整理
[image]	创建时间	2024年3月18日
[image]	**Description**	工具

Little File Explorer 是一款适用于安卓的小巧简单的文件管理器，在设计时充分考虑了兼容性。

▫免费
▫足够小 (< 40KB)
▫满足基本文件操作（剪切、复制、粘贴、重命名、删除）
▫文件名过滤器
▫按名称和修改时间排序
▫ 在SD卡和内部存储之间轻松切换
▫文件/文件夹路径复制
▫最低权限
▫ 暗模式
▫□ MD5校验和生成与验证

□ https://github.com/martinmimigames/little-file-explorer

□ F-Droid: https://f-droid.org/ru/packages/com.martinmimigames.simplefileexplorer/

[image]
[image]

替换掉那些不够安全的插件

[image] 关键词	免追踪 开源 浏览器
[image] 创建时间	2024年3月19日
[image] **Description**	工具

Browser Boost 扩展是一个插件，旨在为众多不够安全的扩展程序提供一种开源的、尊重隐私的替代方案。

功能包括：
▫更改用户代理，以模拟不同的设备或浏览器；
▫在禁止右键单击或选择交互的网站上启用右键单击、复制和选择文本功能；
▫ 添加上下文菜单以将图像保存为JPG、PNG或WebP；
▫禁用 WebRTC 请求以防止 IP 地址泄露 ……

 https://github.com/BrowserBoost/Extension

 https://chromewebstore.google.com/detail/browser-boost-extra-tools/akknpgblpchaoebdoiojonnahhnfgnem

[image]
[image]

替换掉那些不够安全的插件

[image] 关键词		免追踪 开源 浏览器
[image] 创建时间		2024/03/19
[image] **Description**		工具

Browser Boost 扩展是一个插件，旨在为众多不够安全的扩展程序提供一种开源的、尊重隐私的替代方案。

功能包括：
▫更改用户代理，以模拟不同的设备或浏览器；
▫在禁止右键单击或选择交互的网站上启用右键单击、复制和选择文本功能；
▫ 添加上下文菜单以将图像保存为JPG、PNG或WebP；
▫禁用 WebRTC 请求以防止 IP 地址泄露 ……

 https://github.com/BrowserBoost/Extension

 https://chromewebstore.google.com/detail/browser-boost-extra-tools/akknpgblpchaoebdoiojonnahhnfgnem

[image]
[image]

免费的去中心化社交网络平台

[image] 关键词	去中心化 社交网络
[image] 关联	[image]去中心化的社交网络协议；
[image] 创建时间	2024年3月20日
[image] **Description**	工具

Friendica 是一个免费的去中心化社交网络平台。

它将用户连接到一个名为 Fediverse 的联合通信网络。

用户可以与 Friendica、Mastodon、Lemmy、Diaspora、Misskey、Peertube、Pixelfed、Pleroma 等各种平台上的其他人互动。

它还允许用户从 Tumblr、Wordpress 和 RSS 中导入和镜像内容。

用户可以控制内容的隐私设置。

加入Friendica意味着摆脱监视资本家收集数据的束缚。

 https://github.com/friendica/friendica

 公共服务器: https://dir.friendica.social/servers

[image]
[image]

免费的去中心化社交网络平台

[image] 关键词	去中心化 社交网络
[image] 创建时间	2024/03/20
[image] **Description**	工具

Friendica 是一个免费的去中心化社交网络平台。

它将用户连接到一个名为 Fediverse 的联合通信网络。

用户可以与 Friendica、Mastodon、Lemmy、Diaspora、Misskey、Peertube、Pixelfed、Pleroma 等各种平台上的其他人互动。

它还允许用户从 Tumblr、Wordpress 和 RSS 中导入和镜像内容。

用户可以控制内容的隐私设置。

加入Friendica意味着摆脱监视资本家收集数据的束缚。

 https://github.com/friendica/friendica

 公共服务器: https://dir.friendica.social/servers

[image]
[image]

开源笔记应用跨平台

[image]	关键词	离线 笔记
[image]	创建时间	2024年3月22日
[image]	**Description**	工具

Memos 是一款开源笔记应用程序，支持 Markdown 以增强文本格式，可在多种平台上使用。

它通过使用 Go 和 React.js 提供安全的本地存储、快速的纯文本备忘录创建和高性能。

用户可以通过更改服务器名称、图标和描述来个性化应用程序，还可以访问 GitHub 上的代码。

可使用 Docker 部署。

 https://github.com/usememos/memos

[image]
[image]

开源笔记应用跨平台

[image] 关键词	离线 笔记
[image] 创建时间	2024/03/22
[image] **Description**	工具

Memos 是一款开源笔记应用程序，支持 Markdown 以增强文本格式，可在多种平台上使用。

它通过使用 Go 和 React.js 提供安全的本地存储、快速的纯文本备忘录创建和高性能。

用户可以通过更改服务器名称、图标和描述来个性化应用程序，还可以访问 GitHub 上的代码。

可使用 Docker 部署。

 https://github.com/usememos/memos

[image]
[image]

本地托管的 PDF操作工具

[image] 关键词	密码 查询整理 自托管
[image] 创建时间	2024/03/26
[image] **Description**	工具

Stirling-PDF 是一款功能强大的本地托管的基于Web的 PDF操作工具，使用Docker，允许您执行各种PDF操作，如 拆分合并、转换、重组、添加图像、旋转、压缩等等。

所有文件和 PDF 仅存在于客户端，仅在任务执行期间驻留在服务器内存中。用户下载的任何文件都将从服务器中删除。

还包括，添加和删除密码、更改/设置 PDF 权限、添加水印、认证/签署 PDF、编辑元数据、获取 PDF 上的所有信息，以查看或导出为 JSON …… 等等功能。

 https://github.com/Frooodle/Stirling-PDF

[image]
[image]

本地托管的 PDF操作工具

[image] 关键词	密码 查询整理 自托管
[image] 创建时间	2024年3月26日
[image] **Description**	工具

Stirling-PDF 是一款功能强大的本地托管的基于Web的 PDF操作工具，使用Docker，允许您执行各种PDF操作，如 拆分合并、转换、重组、添加图像、旋转、压缩等等。

所有文件和 PDF 仅存在于客户端，仅在任务执行期间驻留在服务器内存中。用户下载的任何文件都将从服务器中删除。

还包括，添加和删除密码、更改/设置 PDF 权限、添加水印、认证/签署 PDF、编辑元数据、获取 PDF 上的所有信息，以查看或导出为 JSON …… 等等功能。

 https://github.com/Frooodle/Stirling-PDF

[image]
[image]

将安卓手机连接到电脑

[image] 关键词	传输安全 加密 安卓
[image] 创建时间	2024年4月3日
[image] **Description**	工具

Device Connect 是一款将安卓手机连接到电脑的工具，类似于KDE Connect。

- 轻量，速度快；
- 带密码的 AES-256 加密；
- 将文件从手机上传到桌面；
- 在桌面上打开手机上的文件和网址；
- 在桌面上显示电话通知；
- 在桌面上执行预定义的命令；
- 定期运行同步任务（目录、联系人、短信）。

 安卓：https://github.com/cyanomiko/dcnnt-android
 PC: https://github.com/cyanomiko/dcnnt-py
 F-Droid: https://f-droid.org/en/packages/net.dcnnt/

[image]
[image]

将安卓手机连接到电脑

[image]	关键词	传输安全 加密 安卓
[image]	创建时间	2024/04/03
[image]	**Description**	工具

Device Connect 是一款将安卓手机连接到电脑的工具，类似于KDE Connect。

▫ 轻量，速度快；
▫ 带密码的 AES-256 加密；
▫ 将文件从手机上传到桌面；
▫ 在桌面上打开手机上的文件和网址；
▫ 在桌面上显示电话通知；
▫ 在桌面上执行预定义的命令；
▫ 定期运行同步任务（目录、联系人、短信）。

□ 安卓：https://github.com/cyanomiko/dcnnt-android
□ PC: https://github.com/cyanomiko/dcnnt-py
□ F-Droid: https://f-droid.org/en/packages/net.dcnnt/

[image]
[image]

一套鼠标和键盘控制多台计算机

[image] 关键词	开源 效率
[image] 创建时间	2024/04/09
[image] **Description**	工具

Lan Mouse 是一款共享鼠标和键盘的程序。

它允许您用一套鼠标和键盘控制多台计算机。就像一个软件 KVM 切换器。

该项目的目标是成为专有工具的开源替代品。

 https://github.com/feschber/lan-mouse

[image]
[image]

一套鼠标和键盘控制多台计算机

[image] 关键词	开源 效率
[image] 创建时间	2024年4月9日
[image] **Description**	工具

Lan Mouse 是一款共享鼠标和键盘的程序。

它允许您用一套鼠标和键盘控制多台计算机。就像一个软件 KVM 切换器。

该项目的目标是成为专有工具的开源替代品。

 https://github.com/feschber/lan-mouse

[image]
[image]

洋葱路由功能的安全信息传递系统

[image] 关键词	tor 传输安全 免追踪 加密
[image] 创建时间	2024/04/15
[image] **Description**	工具

Tinfoil Chat (TFC) 是一个具有洋葱路由功能的安全信息传递系统。

TFC 使用 XChaCha20 - Poly1305 端到端加密技术和可拒绝认证技术来保护发送给个人收件人和群组的所有信息和文件。

TFC 完全通过匿名Tor网络发送所有信息。它使用第三代Tor洋葱服务，提供永远不离开Tor网络的点对点通信。

TFC 还具有流量掩蔽模式，即使用户的网络设备被入侵，也能隐藏通信的类型、数量和时间。

 https://github.com/maqp/tfc

[image]
[image]

洋葱路由功能的安全信息传递系统

[image] 关键词	tor 传输安全 免追踪 加密
[image] 关联	[image]完全Tor
[image] 创建时间	2024年4月15日
[image] **Description**	工具

Tinfoil Chat (TFC) 是一个具有洋葱路由功能的安全信息传递系统。

TFC 使用 XChaCha20 - Poly1305 端到端加密技术和可拒绝认证技术来保护发送给个人收件人和群组的所有信息和文件。

TFC 完全通过匿名Tor网络发送所有信息。它使用第三代Tor洋葱服务，提供永远不离开Tor网络的点对点通信。

TFC 还具有流量掩蔽模式，即使用户的网络设备被入侵，也能隐藏通信的类型、数量和时间。

 https://github.com/maqp/tfc

[image]
[image]

把您的所有消息应用整合在一处

[image] 关键词	IMs 加密 效率 自托管
[image] 创建时间	2024年4月19日
[image] **Description**	工具

Beeper 是一款消息应用聚合器。

只需一个应用，即可与iMessage、WhatsApp、Signal、Telegram 和其他 13 个IMs进行通信。

可以搜索、延迟或存档消息。

是的，通过这里，iMessage 甚至可以在 Android、Windows 和 Linux 上运行。

所有消息经过端对端加密。可自托管您自己的实例。

□ https://www.beeper.com/

[image]
[image]

把您的所有消息应用整合在一处

[image] 关键词	IMs 加密 效率 自托管
[image] 创建时间	2024/04/19
[image] **Description**	工具

Beeper 是一款消息应用聚合器。

只需一个应用，即可与iMessage、WhatsApp、Signal、Telegram 和其他 13 个IMs进行通信。

可以搜索、延迟或存档消息。

是的，通过这里，iMessage 甚至可以在 Android、Windows 和 Linux 上运行。

所有消息经过端对端加密。可自托管您自己的实例。

 https://www.beeper.com/

[image]

检查可疑电子邮件、链接和文件的在线工具

[image] 关键词	URL 电邮 病毒检测 自助
[image] 创建时间	2024年4月23日
[image] **Description**	工具

1. phish.ly - 检查可疑邮件中的URL和附件以判断安全状况。为最终文件创建SHA256和MD5哈希，并提供 VirusTotal 的链接。只需将可疑电子邮件发送到 scan@phish.ly，系统就会自动回复扫描结果。

1. Redirect Detective (https://redirectdetective.com/) – 功能强大的链接分析器，可以找出短链接重定向到哪里、使用了哪个联署网络、检查在哪个阶段设置了 cookies 等等。

1. Is Legit? (https://www.islegitsite.com/) - 检查网站是否合法或是否存在潜在骗局的工具。

1. Hardenize (https://www.hardenize.com/) - 提供任何站点的安全报告：HTTPS、域信息、邮件数据、证书等等。

1. Virus Total (https://www.virustotal.com/gui/home/upload) - 一款最受欢迎的在线病毒检测服务。可检查文件和链接。

1. MetaDefender Cloud (https://metadefender.opswat.com/) - 功能强大的反病毒扫描程序，可扫描文件、链接、IP地址、域

和哈希。

1. Hybrid Analysis (https://www.hybrid-analysis.com/) --一个在线沙箱，您可以在其中检查任何文件。发送文件后，网站会在隔离的 VirtualBox或VMware中运行该文件，观察其在系统中的表现，然后得出结论：该文件是否会对系统造成危害。系统包括 Windows、Linux Ubuntu 和 Android。

1. Dr. Web 是一个机器人，可以通过三种方式检查可疑文件和链接：直接发送消息、从其他聊天工具转发消息，或者直接将机器人添加到聊天工具中，它会在所有媒体和链接传入时自动检查它们。

【额外的】ShrewdEye 是一套实用工具，结合成了一个单一的自动化工作流程，以改善、简化和加快资源发现和漏洞检测。

[image]
[image]

检查可疑电子邮件、链接和文件的在线工具

[image] 关键词	URL 电邮 病毒检测 自助
[image] 创建时间	2024/04/23
[image] **Description**	工具

1. phish.ly - 检查可疑邮件中的URL和附件以判断安全状况。为最终文件创建SHA256和MD5哈希，并提供 VirusTotal 的链接。只需将可疑电子邮件发送到 scan@phish.ly，系统就会自动回复扫描结果。

1. Redirect Detective (https://redirectdetective.com/) – 功能强大的链接分析器，可以找出短链接重定向到哪里、使用了哪个联署网络、检查在哪个阶段设置了 cookies 等等。

1. Is Legit? (https://www.islegitsite.com/) - 检查网站是否合法或是否存在潜在骗局的工具。

1. Hardenize (https://www.hardenize.com/) - 提供任何站点的安全报告：HTTPS、域信息、邮件数据、证书等等。

1. Virus Total (https://www.virustotal.com/gui/home/upload) - 一款最受欢迎的在线病毒检测服务。可检查文件和链接。

1. MetaDefender Cloud (https://metadefender.opswat.com/) - 功能强大的反病毒扫描程序，可扫描文件、链接、IP地址、域

和哈希。

1. Hybrid Analysis (https://www.hybrid-analysis.com/) --一个在线沙箱，您可以在其中检查任何文件。发送文件后，网站会在隔离的 VirtualBox或VMware中运行该文件，观察其在系统中的表现，然后得出结论：该文件是否会对系统造成危害。系统包括 Windows、Linux Ubuntu 和 Android。

1. Dr. Web 是一个机器人，可以通过三种方式检查可疑文件和链接：直接发送消息、从其他聊天工具转发消息，或者直接将机器人添加到聊天工具中，它会在所有媒体和链接传入时自动检查它们。

【额外的】ShrewdEye 是一套实用工具，结合成了一个单一的自动化工作流程，以改善、简化和加快资源发现和漏洞检测。

[image]
[image]

开源零知识加密文件共享

[image]	关键词	传输安全 加密
[image]	创建时间	2024年4月25日
[image]	**Description**	工具

0up 是一种开源的零知识加密文件共享服务。

零知识指的是以高度保密的方式存储、传输或处理数据的在线服务。

文件在上传到兼容的 S3 存储服务之前，会在浏览器端进行加密。

用户可以在自己的环境中克隆、定制和托管自己的0up实例。

 https://github.com/0sumcode/0up

 网站：https://0up.io/

[image]
[image]

开源零知识加密文件共享

[image] 关键词	传输安全 加密
[image] 创建时间	2024/04/25
[image] **Description**	工具

0up 是一种开源的零知识加密文件共享服务。

零知识指的是以高度保密的方式存储、传输或处理数据的在线服务。

文件在上传到兼容的 S3 存储服务之前，会在浏览器端进行加密。

用户可以在自己的环境中克隆、定制和托管自己的0up实例。

 https://github.com/0sumcode/0up

 网站：https://0up.io/

[image]
[image]

安卓加密短信

[image]	关键词	传输安全 加密 安卓 移动设备
[image]	创建时间	2024/05/09
[image]	**Description**	工具

Deku SMS 是一款适用于安卓系统的标准开源短信应用，以隐私和安全为首要原则。

通过该应用您可以发送端到端加密的短信，确保您对话的私密性。

它还具有一项试验性功能，允许您通过短信共享图片，以改善连接受限地区的通信能力。

该应用程序可配置为将短信转发到在线服务器，以便从任何设备快速访问。

 https://github.com/deku-messaging/Deku-SMS-Android

 F-droid: https://f-droid.org/packages/com.afkanerd.deku/

[image]
[image]

从视频或音频中总结对话

[image] 关键词	效率
[image] 创建时间	2024/05/09
[image] **Description**	工具

Speech Condenser 是一款从视频或音频中总结对话的工具。

该流程包括音频提取、说话人二值化、音频分离、语音到文本的转录，以及人工智能辅助摘要。

该工具可用于本地视频文件或 YouTube 视频。

 https://github.com/nezhar/speech-condenser

[image]
[image]

从视频或音频中总结对话

[image]	关键词	效率
[image]	创建时间	2024年5月9日
[image]	**Description**	工具

Speech Condenser 是一款从视频或音频中总结对话的工具。

该流程包括音频提取、说话人二值化、音频分离、语音到文本的转录，以及人工智能辅助摘要。

该工具可用于本地视频文件或 YouTube 视频。

https://github.com/nezhar/speech-condenser

[image]
[image]

安卓加密短信

[image] 关键词	传输安全 加密 安卓 移动设备
[image] 创建时间	2024年5月9日
[image] **Description**	工具

Deku SMS 是一款适用于安卓系统的标准开源短信应用，以隐私和安全为首要原则。

通过该应用您可以发送端到端加密的短信，确保您对话的私密性。

它还具有一项试验性功能，允许您通过短信共享图片，以改善连接受限地区的通信能力。

该应用程序可配置为将短信转发到在线服务器，以便从任何设备快速访问。

 https://github.com/deku-messaging/Deku-SMS-Android

 F-droid: https://f-droid.org/packages/com.afkanerd.deku/

[image]
[image]

在纯文本中隐藏不可见的信息或水印

[image]	关键词	传输安全 隐写术
[image]	创建时间	2024/05/15
[image]	**Description**	工具

Text watermark & Steganography toolkit 是一个用 javascript 编写的十六进制零宽字符文本隐写工具包（可在浏览器中运行）。

它可以在纯文本中隐藏完全不可见的信息或水印。

可以在任何文本中隐藏相当长的隐形信息。

完全本地，不需要互联网连接就能工作，所以在您发送/发布您创建的信息之前，您的数据不会被任何地方捕获。

□ https://github.com/jaceddd/text_watermark

□ 网站: https://rabian.io/text_watermark/

[image]
[image]

安全备份工具

[image]	关键词	加密 备份 数据丢失 查询整理 自托管
[image]	创建时间	2024/05/15
[image]	**Description**	工具

restic 是一款快速、高效、安全的备份程序。

支持 GNU/Linux、macOS、Windows、FreeBSD 和 OpenBSD。

▫ 有许多不同的存储类型，包括自托管和在线服务。
▫ 易于配置和使用，以便在发生数据丢失时可以恢复它。恢复数据非常简单。
▫ 使用加密技术来保证数据的机密性和完整性。
▫ 自动删除重复数据以节省备份空间。

 https://github.com/restic/restic
 https://restic.net/

[image]
[image]

安全备份工具

[image] 关键词	加密 备份 数据丢失 查询整理 自托管
[image] 创建时间	2024年5月15日
[image] **Description**	工具

restic 是一款快速、高效、安全的备份程序。

支持 GNU/Linux、macOS、Windows、FreeBSD 和 OpenBSD。

▫ 有许多不同的存储类型，包括自托管和在线服务。
▫ 易于配置和使用，以便在发生数据丢失时可以恢复它。恢复数据非常简单。
▫ 使用加密技术来保证数据的机密性和完整性。
▫ 自动删除重复数据以节省备份空间。

 https://github.com/restic/restic
 https://restic.net/

[image]
[image]

在纯文本中隐藏不可见的信息或水印

[image] 关键词	传输安全 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2024年5月15日
[image] **Description**	工具

Text watermark & Steganography toolkit 是一个用 javascript 编写的十六进制零宽字符文本隐写工具包（可在浏览器中运行）。

它可以在纯文本中隐藏完全不可见的信息或水印。

可以在任何文本中隐藏相当长的隐形信息。

完全本地，不需要互联网连接就能工作，所以在您发送/发布您创建的信息之前，您的数据不会被任何地方捕获。

 https://github.com/jaceddd/text_watermark

 网站: https://rabian.io/text_watermark/

[image]
[image]

视频隐写术

[image] 关键词	传输安全 加密 隐写术
[image] 创建时间	2024/05/16
[image] **Description**	工具

CryptoFrame 是一款用于视频隐写术的命令行工具。

它允许用户在视频文件中嵌入隐藏的文本信息。

它在CBC模式下使用七级AES-256加密，并受RSA加密的进一步保护。

支持的输入视频格式包括 AVI、MKV、MOV、MP4、OGG、WMV 和 WEBM。

 https://github.com/x011/CryptoFrame

[image]
[image]

视频隐写术

[image] 关键词	传输安全 加密 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2024年5月16日
[image] **Description**	工具

CryptoFrame 是一款用于视频隐写术的命令行工具。

它允许用户在视频文件中嵌入隐藏的文本信息。

它在CBC模式下使用七级AES-256加密，并受RSA加密的进一步保护。

支持的输入视频格式包括 AVI、MKV、MOV、MP4、OGG、WMV 和 WEBM。

 https://github.com/x011/CryptoFrame

[image]
[image]

分析蓝牙环境是否安全

[image] 关键词	反侦察 安卓 监测 自检 防御
[image] 创建时间	2024/05/17
[image] **Description**	工具

Bluetooth Radar 是一款用于分析蓝牙环境的 Android 应用程序。

它可以通知您您正在寻找的设备是否在附近，或者某些未知设备是否已跟踪您很长时间了。

该应用可以将扫描到的设备与已知联系人进行匹配。用户还可以创建设备移动地图。该应用还可以搜索特定时间段内发现的设备。

该应用不会共享您的个人数据或地理位置，所有工作都在离线状态下完成。

 https://github.com/Semper-Viventem/MetaRadar

 F-droid: https://f-droid.org/en/packages/f.cking.software/

[image]
[image]

分析蓝牙环境是否安全

[image]	关键词	反侦察 安卓 监测 自检 防御
[image]	创建时间	2024年5月17日
[image]	**Description**	工具

Bluetooth Radar 是一款用于分析蓝牙环境的 Android 应用程序。

它可以通知您您正在寻找的设备是否在附近，或者某些未知设备是否已跟踪您很长时间了。

该应用可以将扫描到的设备与已知联系人进行匹配。用户还可以创建设备移动地图。该应用还可以搜索特定时间段内发现的设备。

该应用不会共享您的个人数据或地理位置，所有工作都在离线状态下完成。

https://github.com/Semper-Viventem/MetaRadar

F-droid: https://f-droid.org/en/packages/f.cking.software/

[image]
[image]

广告拦截

[image]	关键词	免追踪 浏览器 自助
[image]	创建时间	2024/05/21
[image]	**Description**	工具

uBlock Origin Lite 是 uBlock Origin 开发者新推出的一款实验性扩展，旨在拦截广告。

uBlock Origin Lite (uBOL)扩展遵守 Manifest v3 规则，而且不需要读取/修改网站数据的权限。

uBOL是完全声明式的，这意味着不需要持续的 uBOL 进程来执行过滤，基于 CSS/JS 注入的内容过滤由浏览器本身而非扩展可靠地执行。

这意味着在过滤工作中 uBOL 本身不会占用 CPU/内存资源，只有在您打开弹出面板或是设置页面时才会生成 uBOL 扩展进程。

火狐浏览器：https://addons.mozilla.org/en-GB/firefox/addon/ublock-origin-lite/

谷歌浏览器：https://chromewebstore.google.com/detail/ublock-origin-lite/ddkjiahejlhfcafbddmgiahcphecmpfh

[image]
[image]

广告拦截

[image] 关键词	免追踪 浏览器 自助
[image] 创建时间	2024年5月21日
[image] **Description**	工具

uBlock Origin Lite 是 uBlock Origin 开发者新推出的一款实验性扩展，旨在拦截广告。

uBlock Origin Lite (uBOL)扩展遵守 Manifest v3 规则，而且不需要读取/修改网站数据的权限。

uBOL是完全声明式的，这意味着不需要持续的 uBOL 进程来执行过滤，基于 CSS/JS 注入的内容过滤由浏览器本身而非扩展可靠地执行。

这意味着在过滤工作中 uBOL 本身不会占用 CPU/内存资源，只有在您打开弹出面板或是设置页面时才会生成 uBOL 扩展进程。

火狐浏览器：https://addons.mozilla.org/en-GB/firefox/addon/ublock-origin-lite/

谷歌浏览器：https://chromewebstore.google.com/detail/ublock-origin-lite/ddkjiahejlhfcafbddmgiahcphecmpfh

[image]
[image]

通过临时Wi-Fi 在设备间离线传输文件

[image] 关键词	传输安全 加密 电脑 移动设备
[image] 创建时间	2024年5月27日
[image] **Description**	工具

1、

Flying Carpet 允许您通过临时Wi-Fi 在 Android、iOS、Linux、macOS 和 Windows 设备之间传输文件。

它不需要共享网络或蜂窝网络连接，只需要两台带有Wi-Fi芯片的设备靠近即可。

当U盘无法使用且无法访问无线网络时，或需要在不同文件系统之间移动大文件时，可以使用该工具。

为了安全起见，传输的文件还使用AES协议进行加密。

 https://github.com/spieglt/FlyingCarpet

2、

Airclap - 用于在同一本地网络内的 Mac、iOS、Windows 和 Android 设备之间传输文件。

▫无需联网，无线传输，附近共享。
▫从 airclap.app 或应用程序商店安装。
▫本地网络上可用的最大传输速度。传输过程稳定。

 https://github.com/Gentleflow/Airclap

网站：https://www.airclap.app/

[image]
[image]

通过临时Wi-Fi 在设备间离线传输文件

[image]	关键词	传输安全 加密 电脑 移动设备
[image]	创建时间	2024/05/27
[image]	**Description**	工具

1、

Flying Carpet 允许您通过临时Wi-Fi 在 Android、iOS、Linux、macOS 和 Windows 设备之间传输文件。

它不需要共享网络或蜂窝网络连接，只需要两台带有Wi-Fi芯片的设备靠近即可。

当U盘无法使用且无法访问无线网络时，或需要在不同文件系统之间移动大文件时，可以使用该工具。

为了安全起见，传输的文件还使用AES协议进行加密。

 https://github.com/spieglt/FlyingCarpet

2、

Airclap - 用于在同一本地网络内的 Mac、iOS、Windows 和 Android 设备之间传输文件。

▫无需联网，无线传输，附近共享。
▫从 airclap.app 或应用程序商店安装。
▫本地网络上可用的最大传输速度。传输过程稳定。

 https://github.com/Gentleflow/Airclap

网站：https://www.airclap.app/

[image]
[image]

也是隐写：将敏感信息隐藏在图像中

[image]	关键词	加密 隐写术
[image]	创建时间	2024/06/07
[image]	**Description**	工具

SecretPixel 是一款先进的隐写工具，可将敏感信息隐藏在图像中。

其功能包括使用AES-256和RSA进行加密、压缩、和LSB隐写算法，让嵌入数据更难被检测。

由 Python 编写，可在任何安装了 Python 的系统上使用。

它支持各种图像文件格式，如 PNG、BMP、TGA 和 TIFF。

 https://github.com/x011/SecretPixel

[image]
[image]

也是隐写：将敏感信息隐藏在图像中

[image] 关键词	加密 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2024年6月7日
[image] **Description**	工具

SecretPixel 是一款先进的隐写工具，可将敏感信息隐藏在图像中。

其功能包括使用AES-256和RSA进行加密、压缩、和LSB隐写算法，让嵌入数据更难被检测。

由 Python 编写，可在任何安装了 Python 的系统上使用。

它支持各种图像文件格式，如 PNG、BMP、TGA 和 TIFF。

 https://github.com/x011/SecretPixel

[image]
[image]

加密和匿名发送文件

[image]	关键词	云存储 传输安全 加密
[image]	创建时间	2024/06/11
[image]	**Description**	工具

Internxt Send 是一款用于加密和匿名发送文件的实用工具。

- 不需要注册账户；
- 最大文件大小为 5GB；
- 可通过链接或邮件发送文件；
- 提供付费的加密图库和云存储服务；

 https://send.internxt.com/

[image]
[image]

加密和匿名发送文件

[image] 关键词	云存储 传输安全 加密
[image] 创建时间	2024年6月11日
[image] **Description**	工具

Internxt Send 是一款用于加密和匿名发送文件的实用工具。

- 不需要注册账户；
- 最大文件大小为 5GB；
- 可通过链接或邮件发送文件；
- 提供付费的加密图库和云存储服务；

 https://send.internxt.com/

[image]
[image]

一次性密码和2FA应用

[image] 关键词	2FA 防御
[image] 创建时间	2024/06/13
[image] **Description**	工具

只有密码不一定行，再加一层安全防护吧。

众所周知，无论您的密码有多独特，您都应该尽可能启用双因素身份验证。并且生成基于时间的一次性密码（TOTP）可能会更安全。

1、Owky (https://github.com/charlietango/owky)：
Owky 的优点包括拥有直观的界面和生物识别身份验证功能。缺点是功能较少，可能缺乏开发计划（最后一次修改是在2022年4月）。

2、Tofu (https://tofuauth.com/)：
Tofu 也拥有生物识别身份验证功能，还有与其他设备同步的功能，以及扫描二维码而非插入文本代码来添加新密码的功能。此外，它是用Swift编写的，这是一种专门为iOS/macOS优化的语言。

3、Raivo OTP (https://raivo-otp.com/)：
Raivo 拥有漂亮的界面和 MacOS 客户端，可在设备间同步密码，以及以加密存档形式导出。允许您添加自己的图标并对其进行自定义。

[image]
[image]

一次性密码和2FA应用

[image] 关键词	2FA 防御
[image] 创建时间	2024年6月13日
[image] **Description**	工具

只有密码不一定行，再加一层安全防护吧。

众所周知，无论您的密码有多独特，您都应该尽可能启用双因素身份验证。并且生成基于时间的一次性密码（TOTP）可能会更安全。

1、Owky (https://github.com/charlietango/owky)：
Owky 的优点包括拥有直观的界面和生物识别身份验证功能。缺点是功能较少，可能缺乏开发计划（最后一次修改是在2022年4月）。

2、Tofu (https://tofuauth.com/)：
Tofu 也拥有生物识别身份验证功能，还有与其他设备同步的功能，以及扫描二维码而非插入文本代码来添加新密码的功能。此外，它是用Swift编写的，这是一种专门为iOS/macOS优化的语言。

3、Raivo OTP (https://raivo-otp.com/)：
Raivo 拥有漂亮的界面和 MacOS 客户端，可在设备间同步密码，以及以加密存档形式导出。允许您添加自己的图标并对其进行自定义。

[image]
[image]

去除图像中的水印和其他元素

[image] 关键词	数字足迹 自助
[image] 创建时间	2024年6月15日
[image] **Description**	工具

1. iMyFone MarkGo (https://filme.imyfone.com/watermark-remover) - 可去除图片和视频中的水印。

1. Aiseesoft Free Watermark Remover (https://www.aiseesoft.com/watermark-remover-online) - 免费在线工具，使用 AI。

1. Watermarkremover (https://www.watermarkremover.io/zh) - 另一款免费在线去水印工具。

1. Inpaint (https://theinpaint.com) - 免费工具，有桌面版和在线版。

1. Fotophire Photo Eraser (https://photo.wondershare.com/photo-eraser.html) - 桌面版，简单但功能强大的照片编辑器。有试用版。

1. TouchRemove (https://play.google.com/store/apps/details?id=com.genewarrior.touchremove2&hl=en_US&gl=US) - Android 上的类似应用程序，不仅可以删除，还可以移动照片上的对象。

1. Downloader.la (http://downloader.la) - 从 Getty Images、Adobe Stock 和 DepositPhotos 下载无水印图片。

1. Hama (https://www.hama.app/en) - 同样使用神经网络去除照片中的制定物体。

[image]
[image]

去除图像中的水印和其他元素

[image] 关键词	数字足迹 自助
[image] 创建时间	2024/06/15
[image] Description	工具

1. iMyFone MarkGo (https://filme.imyfone.com/watermark-remover) - 可去除图片和视频中的水印。

1. Aiseesoft Free Watermark Remover (https://www.aiseesoft.com/watermark-remover-online) - 免费在线工具，使用 AI。

1. Watermarkremover (https://www.watermarkremover.io/zh) - 另一款免费在线去水印工具。

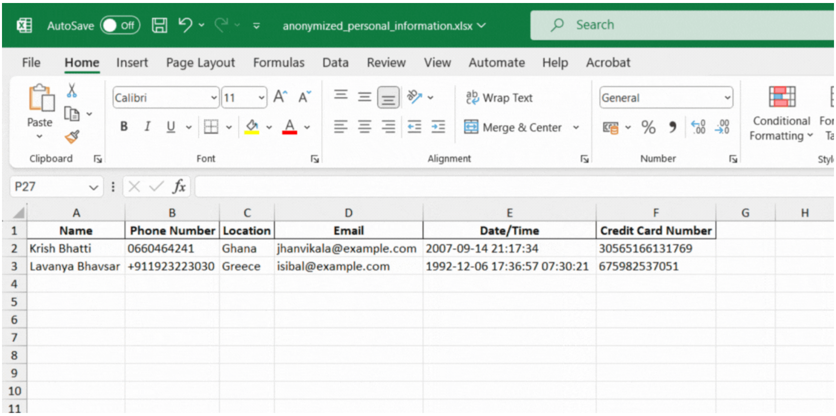
1. Inpaint (https://theinpaint.com) - 免费工具，有桌面版和在线版。

1. Fotophire Photo Eraser (https://photo.wondershare.com/photo-eraser.html) - 桌面版，简单但功能强大的照片编辑器。有试用版。

1. TouchRemove (https://play.google.com/store/apps/details?id=com.genewarrior.touchremove2&hl=en_US&gl=US) - Android 上的类似应用程序，不仅可以删除，还可以移动照片上的对象。

1. Downloader.la (http://downloader.la) - 从 Getty Images、Adobe Stock 和 DepositPhotos 下载无水印图片。

1. Hama (https://www.hama.app/en) - 同样使用神经网络去除照片中的制定物体。



	A	B	C	D	E	F
1	Name	Phone Number	Location	Email	Date/Time	Credit Card Number
2	Krish Bhatti	0660464241	Ghana	jhanvikala@example.com	2007-09-14 21:17:34	30565166131769
3	Lavanya Bhavsar	+911923223030	Greece	isibal@example.com	1992-12-06 17:36:57 07:30:21	675982537051

[image]

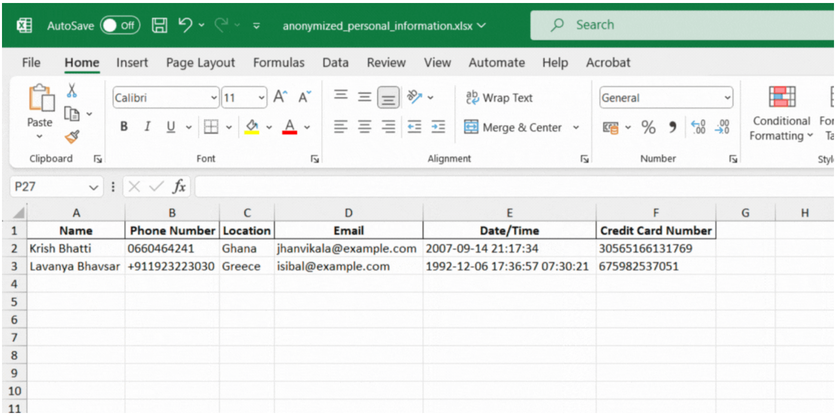
对文件中的敏感数据匿名化

[image]	关键词	反侦察 预防性
[image]	创建时间	2024年6月17日
[image]	**Description**	工具

Anonymize Excel - 这是一个 Python 脚本，用于对 Excel 文件中的数据进行匿名化。

它有助于匿名化敏感数据以保护隐私，如信用卡号、姓名、地点等等。

☐ https://github.com/Welding-Torch/Anonymize_Excel



Name	Phone Number	Location	Email	Date/Time	Credit Card Number
Krish Bhatti	0660464241	Ghana	jhanvikala@example.com	2007-09-14 21:17:34	30565166131769
Lavanya Bhavsar	+911923223030	Greece	isibal@example.com	1992-12-06 17:36:57 07:30:21	675982537051

[image]

对文件中的敏感数据匿名化

[image] 关键词 反侦察 预防性

[image] 创建时间 2024/06/17

[image] **Description** 工具

Anonymize Excel - 这是一个 Python 脚本，用于对 Excel 文件中的数据进行匿名化。

它有助于匿名化敏感数据以保护隐私，如信用卡号、姓名、地点等等。

□ https://github.com/Welding-Torch/Anonymize_Excel

[image]
[image]

安卓加密图库

[image]	关键词	加密 安卓 查询整理
[image]	创建时间	2024年6月19日
[image]	**Description**	工具

Valv 是一款适用于安卓设备的加密图库存储工具。

支持图片、GIF和视频；使用文件夹进行组织；无需权限；加密文件存储在磁盘上，以便在设备之间轻松备份和传输；通过使用不同的密码支持多个保管库 ……

文件加密使用ChaCha20，密钥使用 PBKDF2 和 HMAC-SHA512。

需要安卓9级以上版本。

 https://github.com/Arctosoft/Valv-Android

F-dorid: https://f-droid.org/en/packages/se.arctosoft.vault/

[image]
[image]

安卓加密图库

[image]	关键词	加密 安卓 查询整理
[image]	创建时间	2024/06/19
[image]	**Description**	工具

Valv 是一款适用于安卓设备的加密图库存储工具。

支持图片、GIF和视频；使用文件夹进行组织；无需权限；加密文件存储在磁盘上，以便在设备之间轻松备份和传输；通过使用不同的密码支持多个保管库 ......

文件加密使用ChaCha20，密钥使用 PBKDF2 和 HMAC-SHA512。

需要安卓9级以上版本。

 https://github.com/Arctosoft/Valv-Android

F-dorid: https://f-droid.org/en/packages/se.arctosoft.vault/

[image]
[image]

安全共享

[image] 关键词		传输安全 加密
[image] 创建时间		2024/06/21
[image] **Description**		工具

FlashPaper 是一款一次性加密的零知识密码/秘密共享应用程序，注重简单性和安全性。

无需数据库或复杂配置。

可以使用 Docker 或传统的 PHP 7.0+ 和Web服务器进行安装。

该应用程序的工作原理是生成随机密钥，使用 bcrypt 散列并加密用户发送的文本。

使用相应的密钥对提交的文本进行解密即可。

 https://github.com/AndrewPaglusch/FlashPaper

演示：https://flashpaper.io/

[image]
[image]

安全共享

[image] 关键词	传输安全 加密
[image] 关联	[image]在不安全渠道上尽可能安全地共享秘密 ；[image]安全的秘密共享 ；[image]点对点文件传输 ；[image]在不同操作系统之间传输文件 ；[image]一些私密安全的文件传输解决方案 ；[image]在任何聊天工具中发送端对端加密信息 ；
[image] 创建时间	2024年6月21日
[image] **Description**	工具

FlashPaper 是一款一次性加密的零知识密码/秘密共享应用程序，注重简单性和安全性。

无需数据库或复杂配置。

可以使用 Docker 或传统的 PHP 7.0＋ 和Web服务器进行安装。

该应用程序的工作原理是生成随机密钥，使用 bcrypt 散列并加密用户发送的文本。

使用相应的密钥对提交的文本进行解密即可。

 https://github.com/AndrewPaglusch/FlashPaper

演示：https://flashpaper.io/

[image]
[image]

完全本地化的开源密码保管

[image] 关键词	加密 安卓 密码 自托管
[image] 创建时间	2024/06/24
[image] **Description**	工具

LocalLock 是一款 Android 应用程序，其唯一目的是创建一个安全的、完全本地化的开源密码保管应用。

▫ 简单的用户界面
▫生物识别验证

▫ 所有数据都在本地存储
▫没有第三方集成（没有广告，没有跟踪，没有分析）
▫离线工作
▫ 使用锁屏 PIN 码进行保护（可选）
▫ 密码在存储之前使用 AES-256 进行加密
▫ 轻松将密码复制到剪贴板

 https://github.com/PriyavKaneria/LocalLock

[image]
[image]

完全本地化的开源密码保管

[image] 关键词	加密 安卓 密码 自托管
[image] 创建时间	2024年6月24日
[image] **Description**	工具

LocalLock 是一款 Android 应用程序，其唯一目的是创建一个安全的、完全本地化的开源密码保管应用。

▫ 简单的用户界面
▫生物识别验证

▫ 所有数据都在本地存储
▫没有第三方集成（没有广告，没有跟踪，没有分析）
▫离线工作
▫ 使用锁屏 PIN 码进行保护（可选）
▫ 密码在存储之前使用 AES-256 进行加密
▫ 轻松将密码复制到剪贴板

 https://github.com/PriyavKaneria/LocalLock

[image]
[image]

在任何聊天工具中发送算对端加密信息

[image] 关键词	IMs 传输安全 加密
[image] 创建时间	2024年6月27日
[image] **Description**	工具

KryptEY 是一款安卓键盘，可在任何聊天工具中通过Signal协议发送安全的端到端加密信息。

无论法律状况如何，也无论您的聊天工具是否使用 E2EE，都能安全独立地进行通信。无需服务器。

▫通过键盘中的单独文本字段输入消息
▫使用剪贴板读取消息
▫消息的加密/解密
▫用于查看已发送/已接收消息的日志
▫深浅主题
以及更多...

 https://github.com/amnesica/KryptEY

 IzzyOnDroid: https://android.izzysoft.de/repo/apk/com.amnesica.kryptey

[image]
[image]

在任何聊天工具中发送算对端加密信息

[image] 关键词		IMs 传输安全 加密
[image] 创建时间		2024/06/27
[image] **Description**		工具

KryptEY 是一款安卓键盘，可在任何聊天工具中通过Signal协议发送安全的端到端加密信息。

无论法律状况如何，也无论您的聊天工具是否使用 E2EE，都能安全独立地进行通信。无需服务器。

▫通过键盘中的单独文本字段输入消息
▫使用剪贴板读取消息
▫消息的加密/解密
▫用于查看已发送/已接收消息的日志
▫深浅主题
以及更多...

 https://github.com/amnesica/KryptEY

 IzzyOnDroid: https://android.izzysoft.de/repo/apk/com.amnesica.kryptey

[image]
[image]

自动检查病毒，并替换为安全版本

[image] 关键词	病毒检测 自主
[image] 创建时间	2024年7月1日
[image] **Description**	工具

Dangerzone - 检查各种可能有危险的文件并将其转换为安全版本。

Mac、Windows 或 Linux 计算机适用。

可以用它来打开各种类型的文档：PDF、Microsoft Office 或 LibreOffice 文档或图像。即使原始文档很危险并且通常会入侵您的计算机，Dangerzone 也会将其转换为您可以打开和阅读的安全 PDF。

 https://dangerzone.rocks/

[image]
[image]

临时电邮

[image] 关键词	免追踪 电邮
[image] 创建时间	2024/07/01
[image] **Description**	工具

TempMail 是一款网络应用程序，用于创建临时电子邮件地址并接收邮件。

它使用的是 1secmail API。

功能包括创建新的临时电子邮件地址、下载电子邮件、查看邮件和下载附件。

 https://github.com/mehmetkahya0/temp-mail

[image]
[image]

自动检查病毒，并替换为安全版本

[image] 关键词	病毒检测 自主
[image] 创建时间	2024/07/01
[image] **Description**	工具

Dangerzone - 检查各种可能有危险的文件并将其转换为安全版本。

Mac、Windows 或 Linux 计算机适用。

可以用它来打开各种类型的文档：PDF、Microsoft Office 或 LibreOffice 文档或图像。即使原始文档很危险并且通常会入侵您的计算机，Dangerzone 也会将其转换为您可以打开和阅读的安全 PDF。

 https://dangerzone.rocks/

[image]
[image]

临时电邮

[image] 关键词		免追踪 电邮
[image] 创建时间		2024年7月1日
[image] **Description**		工具

TempMail 是一款网络应用程序，用于创建临时电子邮件地址并接收邮件。

它使用的是 1secmail API。

功能包括创建新的临时电子邮件地址、下载电子邮件、查看邮件和下载附件。

 https://github.com/mehmetkahya0/temp-mail

[image]
[image]

隐私型安卓网页浏览器

[image] 关键词	免追踪 安卓 数字足迹 浏览器 移动设备
[image] 创建时间	2024年7月11日
[image] **Description**	工具

FREE Browser 是一款注重隐私保护的、开源、且不含跟踪工具的安卓网页浏览器。

▫AdBlocker 使用 StevenBlack 主机列表
▫防止浏览器指纹识别
▫Cookie Banner Blocker：自动拒绝
▫自定义 JavaScript、cookie 和 DOM 存储（基于域/书签）
▫支持 Greasemonkey 样式脚本
▫针对单手操作进行了优化
▫另存为PDF
以及更多...

https://github.com/woheller69/browser

F-droid: https://f-droid.org/packages/org.woheller69.browser/

[image]
[image]

隐私型安卓网页浏览器

[image]	关键词	免追踪 安卓 数字足迹 浏览器 移动设备
[image]	创建时间	2024/07/11
[image]	**Description**	工具

FREE Browser 是一款注重隐私保护的、开源、且不含跟踪工具的安卓网页浏览器。

▫AdBlocker 使用 StevenBlack 主机列表
▫防止浏览器指纹识别
▫Cookie Banner Blocker：自动拒绝
▫自定义 JavaScript、cookie 和 DOM 存储（基于域/书签）
▫支持 Greasemonkey 样式脚本
▫针对单手操作进行了优化
▫另存为PDF
以及更多...

https://github.com/woheller69/browser

F-droid: https://f-droid.org/packages/org.woheller69.browser/

[image]
[image]

安全地隐藏和加密文件

[image]	关键词	传输安全 加密 反侦察 隐写术
[image]	创建时间	2024/07/15
[image]	**Description**	工具

File Hider 允许您使用多层AES-256加密技术在另一个文件中安全地隐藏和加密文件。AES密钥本身使用RSA加密。

特点：

- 多层加密： 每个文件用AES-256加密七次，以提高安全性。
- RSA加密： AES密钥使用RSA加密，确保只有私钥持有者才能解密隐藏文件。
- 安全隐藏： 加密文件隐藏在另一个文件中，很难发现隐藏文件的存在。
- 保留文件名： 保留原始文件名，解密后可恢复原始文件名。
- 重命名选项： 提供在解隐过程中保存原始文件前重命名文件的功能。
- 命令行支持： 允许通过命令行参数隐藏和解除隐藏文件。

- 加密前压缩：提高存储效率。

- 对加密数据进行Base64编码： 确保安全存储和传输，降低取证工具的可探测性。

 https://github.com/x011/File_Hider

[image]
[image]

安全地隐藏和加密文件

[image] 关键词	传输安全 加密 反侦察 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2024年7月15日
[image] Description	工具

File Hider 允许您使用多层AES-256加密技术在另一个文件中安全地隐藏和加密文件。AES密钥本身使用RSA加密。

特点：

- 多层加密： 每个文件用AES-256加密七次，以提高安全性。
- RSA加密： AES密钥使用RSA加密，确保只有私钥持有者才能解密隐藏文件。
- 安全隐藏： 加密文件隐藏在另一个文件中，很难发现隐藏文件的存在。
- 保留文件名： 保留原始文件名，解密后可恢复原始文件名。
- 重命名选项： 提供在解隐过程中保存原始文件前重命名文件的功能。
- 命令行支持： 允许通过命令行参数隐藏和解除隐藏文件。

- 加密前压缩：提高存储效率。
- 对加密数据进行Base64编码： 确保安全存储和传输，降低取证工具的可探测性。

 https://github.com/x011/File_Hider

[image]
[image]

安卓开源短信网关

[image] 关键词	SMS 安卓 移动设备
[image] 创建时间	2024年7月18日
[image] **Description**	工具

extBee 是一个开源短信网关，允许用户使用 REST API 从Web应用程序发送SMS消息。

安卓手机可用作SMS网关。

 https://github.com/vernu/textbee

网站：https://textbee.dev/

[image]
[image]

安卓开源短信网关

[image] 关键词	SMS 安卓 移动设备
[image] 创建时间	2024/07/18
[image] **Description**	工具

extBee 是一个开源短信网关，允许用户使用 REST API 从Web应用程序发送SMS消息。

安卓手机可用作SMS网关。

 https://github.com/vernu/textbee

网站：https://textbee.dev/

[image]
[image]

开源 2FA 应用

[image] 关键词	2FA 加密 密码
[image] 创建时间	2024/07/25
[image] **Description**	工具

Wristkey 是一款适用于 Wear OS 和安卓智能手表的开源 2FA 应用程序。

它无需将手表与手机配对即可使用。

支持从 Aegis Authenticator、OTP 和 Bitwarden 导入和导出。

具有屏幕锁定、本地存储加密和通过 Wi-Fi 加密传输的功能。

支持各种OTP模式，支持圆形和方形设备。

 https://github.com/0x4f53/Wristkey

[image]
[image]

开源 2FA 应用

[image]	关键词	2FA 加密 密码
[image]	创建时间	2024年7月25日
[image]	**Description**	工具

Wristkey 是一款适用于 Wear OS 和安卓智能手表的开源 2FA 应用程序。

它无需将手表与手机配对即可使用。

支持从 Aegis Authenticator、OTP 和 Bitwarden 导入和导出。

具有屏幕锁定、本地存储加密和通过 Wi-Fi 加密传输的功能。

支持各种OTP模式，支持圆形和方形设备。

 https://github.com/0x4f53/Wristkey

[image]
[image]

以更私密简洁的方式浏览 Twitter/X

[image] 关键词		免追踪 社交网络
[image] 创建时间		2024年7月26日
[image] **Description**		工具

Quacker 是一款 Android 应用程序，旨在成为一种更私密、更简洁的 Twitter/X 浏览方式。

功能包括书签、趋势、深浅色主题、订阅/List、投票、搜索等等。

 https://github.com/TheHCJ/Quacker

F-droid: https://f-droid.org/en/packages/com.thehcj.quacker/

[image]
[image]

以更私密简洁的方式浏览 Twitter/X

[image]	关键词	免追踪 社交网络
[image]	创建时间	2024/07/26
[image]	**Description**	工具

Quacker 是一款 Android 应用程序，旨在成为一种更私密、更简洁的 Twitter/X 浏览方式。

功能包括书签、趋势、深浅色主题、订阅/List、投票、搜索等等。

 https://github.com/TheHCJ/Quacker

F-droid: https://f-droid.org/en/packages/com.thehcj.quacker/

[image]
[image]

安全存储和身份验证管理

[image]	关键词	2FA 密码 身份验证
[image]	创建时间	2024/07/29
[image]	**Description**	工具

TLock 是一款用于安全存储和管理身份验证令牌的开源工具。

它能集中创建和维护基于时间的一次性密码（TOTP）和其他类型的令牌。

其功能包括跨平台兼容性、支持多用户密码保护、可自定义的密钥绑定、在文件夹中组织令牌、多种主题、可显示发行方图标。

 https://github.com/eklairs/tlock

[image]
[image]

安全存储和身份验证管理

[image] 关键词	2FA 密码 身份验证
[image] 创建时间	2024年7月29日
[image] **Description**	工具

TLock 是一款用于安全存储和管理身份验证令牌的开源工具。

它能集中创建和维护基于时间的一次性密码（TOTP）和其他类型的令牌。

其功能包括跨平台兼容性、支持多用户密码保护、可自定义的密钥绑定、在文件夹中组织令牌、多种主题、可显示发行方图标。

 https://github.com/eklairs/tlock

[image]
[image]

开源协作式书签管理器

[image]	关键词	云存储 团队 自托管
[image]	创建时间	2024/08/05
[image]	**Description**	工具

Linkwarden 是一款独立的开源协作式书签管理器。

Linkwarden 允许用户收集、组织和归档网页。它能将每个网页的副本保存为截图和 PDF 文件，即使原始内容已不可用，也能确保其可访问性。

Linkwarden 还采用了自适应设计，支持深色和浅色模式。该软件还包括一个浏览器扩展，并能从其他平台轻松导入和导出书签。

该软件支持自托管，但也提供具有高级功能的云服务。

 https://github.com/linkwarden/linkwarden

网站：https://linkwarden.app/

[image]
[image]

开源协作式书签管理器

[image] 关键词	云存储 团队 自托管
[image] 创建时间	2024年8月5日
[image] **Description**	工具

Linkwarden 是一款独立的开源协作式书签管理器。

Linkwarden 允许用户收集、组织和归档网页。它能将每个网页的副本保存为截图和 PDF 文件，即使原始内容已不可用，也能确保其可访问性。

Linkwarden 还采用了自适应设计，支持深色和浅色模式。该软件还包括一个浏览器扩展，并能从其他平台轻松导入和导出书签。

该软件支持自托管，但也提供具有高级功能的云服务。

 https://github.com/linkwarden/linkwarden

网站：https://linkwarden.app/

[image]
[image]

更安全的实时视频会议平台

[image]	关键词	团队 效率
[image]	创建时间	2024年8月6日
[image]	**Description**	工具

MiroTalk SFU 是一个用于实时视频会议的免费开源 WebRTC 平台。

支持 4K分辨率，兼容所有主流浏览器和平台。

其功能包括无限会议室、实时流媒体、133种语言翻译、会议室密码保护、屏幕共享、文件共享、可定义的用户界面主题、REST API 集成等。

用户可以直接加入会议室、 使用特定链接或二维码。

 https://github.com/miroslavpejic85/mirotalksfu

网站：https://sfu.mirotalk.com/

[image]
[image]

更安全的实时视频会议平台

[image]	关键词	团队 效率
[image]	创建时间	2024/08/06
[image]	**Description**	工具

MiroTalk SFU 是一个用于实时视频会议的免费开源 WebRTC 平台。

支持 4K分辨率，兼容所有主流浏览器和平台。

其功能包括无限会议室、实时流媒体、133种语言翻译、会议室密码保护、屏幕共享、文件共享、可定义的用户界面主题、REST API 集成等。

用户可以直接加入会议室、 使用特定链接或二维码。

 https://github.com/miroslavpejic85/mirotalksfu

网站：https://sfu.mirotalk.com/

[image]
[image]

一些私密安全的文件传输解决方案

[image] 关键词	传输安全 加密
[image] 关联	[image]在不安全渠道上尽可能安全地共享秘密 ；[image]安全的秘密共享 ；[image]点对点文件传输 ；[image]在不同操作系统之间传输文件 ；[image]安全共享 ；
[image] 创建时间	2024年8月8日
[image] Description	工具

1. OnionShare 2.3.1 - 开源工具，可为任何大小的文件提供安全的匿名共享；（https://onionshare.org/ ）

1. Blindsend - 采用端到端加密的安全文件共享工具；（https://github.com/blindnet-io/blindsend ）

1. croc - 允许任意两台电脑之间简单安全地共享文件的工具。这是同类产品中唯一的 CLI 文件共享工具；（https://github.com/schollz/croc ）

1. Wormhole - 另一种无需注册即可发送加密文件的服务。作者可能是魔法虫洞的铁粉；（https://wormhole.app/ ）

1. Catbox - 一种匿名文件共享服务。禁止上传 .exe、.scr、.cpl、.doc、.jar 文件；（https://catbox.moe/ ）

1. Surge -- 用于匿名文件共享的独特客户端；（https://

github.com/rule110-io/surge ）

1. Sendfiles.online - 一种通过随机密码发送加密文件的服务；（https://sendfilesencrypted.com/ ）

1. Blaze - 另一种安全发送文件的服务；（https://blaze.vercel.app/）

更多：
Portal：https://github.com/SpatiumPortae/portal
Winden：https://winden.app/s
Pairdrop：https://github.com/schlagmichdoch/PairDrop

[image]
[image]

一些私密安全的文件传输解决方案

[image] 关键词	传输安全 加密
[image] 创建时间	2024/08/08
[image] **Description**	工具

1. OnionShare 2.3.1 - 开源工具，可为任何大小的文件提供安全的匿名共享；（https://onionshare.org/ ）

1. Blindsend - 采用端到端加密的安全文件共享工具；（https://github.com/blindnet-io/blindsend ）

1. croc - 允许任意两台电脑之间简单安全地共享文件的工具。这是同类产品中唯一的 CLI 文件共享工具；（https://github.com/schollz/croc ）

1. Wormhole - 另一种无需注册即可发送加密文件的服务。作者可能是魔法虫洞的铁粉；（https://wormhole.app/ ）

1. Catbox - 一种匿名文件共享服务。禁止上传.exe、.scr、.cpl、.doc、.jar 文件；（https://catbox.moe/ ）

1. Surge -- 用于匿名文件共享的独特客户端；（https://github.com/rule110-io/surge ）

1. Sendfiles.online - 一种通过随机密码发送加密文件的服务；（https://sendfilesencrypted.com/ ）

1. Blaze - 另一种安全发送文件的服务；（https://blaze.vercel.app/）

更多：
Portal：https://github.com/SpatiumPortae/portal
Winden：https://winden.app/s
Pairdrop：https://github.com/schlagmichdoch/PairDrop

[image]
[image]

硬件密码管理器

[image]	关键词	密码 身份验证
[image]	创建时间	2024/08/19
[image]	**Description**	工具

PasswordPump - 基于 Arduino 的硬件密码管理器。

最多可存储 254 个账户（账户名 + 登录名 + 密码）。数据存储在两个可移动存储芯片上，采用AES128加密。

该设备通过USB电缆与电脑连接。要访问该设备（其中保存的所有账户），需要输入主密码。然后，在列表中选择所需的账户，并将光标放在电脑上的输入表单中。密码管理器本身会将授权数据输入电脑。

 https://github.com/seawarrior181/PasswordPump/

[image]
[image]

硬件密码管理器

[image]	关键词	密码 身份验证
[image]	创建时间	2024年8月19日
[image]	**Description**	工具

PasswordPump - 基于 Arduino 的硬件密码管理器。

最多可存储 254 个账户（账户名 + 登录名 + 密码）。数据存储在两个可移动存储芯片上，采用AES128加密。

该设备通过USB电缆与电脑连接。要访问该设备（其中保存的所有账户），需要输入主密码。然后，在列表中选择所需的账户，并将光标放在电脑上的输入表单中。密码管理器本身会将授权数据输入电脑。

 https://github.com/seawarrior181/PasswordPump/

[image]
[image]

安全消息应用

[image] 关键词	IMs 加密 身份验证
[image] 创建时间	2024年8月23日
[image] **Description**	工具

PrivatePing 是一个基于 Python Django 框架的安全消息应用。

提供端到端加密、匿名登录和安全身份验证。

 https://github.com/princekhunt/privateping

实时演示： https://privateping.plutoweb.live/

[image]
[image]

安全消息应用

[image]	关键词	IMs 加密 身份验证
[image]	创建时间	2024/08/23
[image]	**Description**	工具

PrivatePing 是一个基于 Python Django 框架的安全消息应用。

提供端到端加密、匿名登录和安全身份验证。

 https://github.com/princekhunt/privateping

实时演示： https://privateping.plutoweb.live/

[image]
[image]

检查密码是否泄漏

[image]	关键词	密码 自检
[image]	创建时间	2024/08/24
[image]	**Description**	工具

Password Monitor - 这款 Android 应用程序与 Have I Been Pwned? 无缝集成，可帮助您检查密码是否在任何公开披露的数据泄漏中。

 https://github.com/StellarSand/Password-Monitor

F-droid: https://f-droid.org/packages/com.password.monitor/

[image]
[image]

检查密码是否泄漏

[image]	关键词	密码 自检
[image]	创建时间	2024年8月24日
[image]	**Description**	工具

Password Monitor - 这款 Android 应用程序与 Have I Been Pwned? 无缝集成，可帮助您检查密码是否在任何公开披露的数据泄漏中。

 https://github.com/StellarSand/Password-Monitor

F-droid: https://f-droid.org/packages/com.password.monitor/

[image]
[image]

隐私型电邮提供商的列表

[image] 关键词	免追踪 加密 暗网 电邮
[image] 创建时间	2024/08/30
[image] **Description**	工具

这里是一份隐私型电邮提供商的列表，包括明网和暗网服务。其中有些提供自动加密功能，有些则需要手动设置，您可以根据以下列出的相关信息选择适合您的。

1. ProtonMail

- 🌍 地点：瑞士。
- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，可选付费。
- 🎤 网站： ProtonMail

1. CyberFear
    - 🌍 位置： 未知。

- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，付费可选。
- 🖊 网站： CyberFear

1. Tutanota

- 🌍地点：德国。
- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，付费可选。
- 🖊 网站： Tutanota

1. CounterMail

- 🌍地点：瑞典。
- 🔑 加密： 是（需手动设置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费 30 天，然后可选择付费。
- 🖊 网站： CounterMail

1. Paranoid Email

- 🌍 地点： 未知。
- 🔑 加密： 是（在电子邮件客户端上手动设置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，需要邀请。
- 🔗 网站： [Paranoid Email]（HTTPS://Paranoid.Email/）

1. SwisMail

- 🌍地点： 瑞士。
- 🔑 加密： 是（需设置）。
- 🔐 2SV/2FA：不确定。
- 💸 免费还是付费服务？免费注册，可选择付费升级。
- 🔗 网站： [SwisMail]（HTTPS://SwisMail.Com/）

1. NeoMailBox

- 🌍地点：瑞士。
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：不确定。

- 💸 免费还是付费服务？付费。
- 🔗 网站： NeoMailBox

1. Secure E-Mail

- 🌍地点： 未知（可能是土耳其）。
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：不确定。
- 💸 免费还是付费服务？付费。
- 🔗 网站： 安全电子邮件

1. Private Mail

- 🌍 地点： 美国。
- 🔑 加密： 是（需手动设置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，可选择付费。
- 🔗 网站： [Private Mail

1. LavaBit

- 🌍地点：美国.
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：不确定。
- 💸 免费还是付费服务？付费。
- 🔗 网站： LavaBit

1. DarkMail

- 🌍 地点： 美国。
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：未知。
- 💸 免费还是付费服务？未知。
- 🔗 网站： DarkMail（尚未发布）

1. SwissCow

- 🌍 地点：瑞士。
- 🔑 加密： 未知。
- 🔐 2SV/2FA：未知。

- 💸 免费还是付费服务？未知。

- 🔗 网站： SwissCow

[image]
[image]

隐私型电邮提供商的列表

[image] 关键词	免追踪 加密 暗网 电邮
[image] 关联	[image]一些较安全的电邮客户端选项
[image] 创建时间	2024年8月30日
[image] **Description**	工具

这里是一份隐私型电邮提供商的列表，包括明网和暗网服务。其中有些提供自动加密功能，有些则需要手动设置，您可以根据以下列出的相关信息选择适合您的。

1. ProtonMail

- 🌍 地点：瑞士。
- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，可选付费。
- 🖋 网站： ProtonMail

1. CyberFear
    - 🌍 位置： 未知。

- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，付费可选。
- 🔗 网站： CyberFear

1. Tutanota

- 🌍地点：德国。
- 🔑 加密： 是（自动内置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，付费可选。
- 🔗 网站： Tutanota

1. CounterMail

- 🌍地点：瑞典。
- 🔑 加密： 是（需手动设置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费 30 天，然后可选择付费。
- 🔗 网站： CounterMail

1. Paranoid Email

    - 🌍 地点： 未知。
    - 🔑 加密： 是（在电子邮件客户端上手动设置）。
    - 🔐 2SV/2FA：是。
    - 💸 免费还是付费服务？免费，需要邀请。
    - 🖋 网站： [Paranoid Email]（HTTPS://Paranoid.Email/）

1. SwisMail

    - 🌍地点： 瑞士。
    - 🔑 加密： 是（需设置）。
    - 🔐 2SV/2FA：不确定。
    - 💸 免费还是付费服务？免费注册，可选择付费升级。
    - 🖋 网站： [SwisMail]（HTTPS://SwisMail.Com/）

1. NeoMailBox

    - 🌍地点：瑞士。
    - 🔑 加密： 是（设置方法不清楚）。
    - 🔐 2SV/2FA：不确定。

    - 💸 免费还是付费服务？付费。
    - 🔗 网站： NeoMailBox

1. Secure E-Mail

- 🌍地点： 未知（可能是土耳其）。
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：不确定。
- 💸 免费还是付费服务？付费。
- 🔗 网站： 安全电子邮件

1. Private Mail

- 🌍 地点： 美国。
- 🔑 加密： 是（需手动设置）。
- 🔐 2SV/2FA：是。
- 💸 免费还是付费服务？免费，可选择付费。
- 🔗 网站： [Private Mail

1. LavaBit

- 🌍地点：美国.
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：不确定。
- 💸 免费还是付费服务？付费。
- 🔗 网站： LavaBit

1. DarkMail

- 🌍 地点： 美国。
- 🔑 加密： 是（设置方法不清楚）。
- 🔐 2SV/2FA：未知。
- 💸 免费还是付费服务？未知。
- 🔗 网站： DarkMail（尚未发布）

1. SwissCow

- 🌍 地点：瑞士。
- 🔑 加密： 未知。
- 🔐 2SV/2FA：未知。

- 💸 免费还是付费服务？未知。
- 🔗 网站： SwissCow

[image]
[image]

从明网搜索 Tor

[image]	关键词	tor
[image]	创建时间	2024年9月3日
[image]	**Description**	工具

1. ahmia.fi (https://ahmia.fi/) - 最著名的开源暗网搜索引擎之一的明网镜像；

1. onionengine.com (https://onionengine.com/)- 同上，只是该搜索引擎不那么热门；

1. darkhunt.net (https://darkhunt.net/)- 另一个在明网中搜索洋葱网站的工具，很有效，但有很多广告；

1. Thehiddenwiki.com (thehiddenwiki.com) - 古老的链接目录；

1. onionland.io (https://onionland.io/) - 在 Tor2Web 的支持下创建的搜索引擎。

当然您还可以谷歌“site:onion.ly”，也能找到不少 .onion 网站，但不建议在谷歌上搜索这类资源。
也同样不建议您使用明网工具搜索风险过高的暗网内容，原因一样。

更推荐本站曾经推荐过的暗网搜索引擎，通过在本站搜索 #tor 标签可找到它们。

[image]
[image]

从明网搜索 Tor

[image]	关键词	tor
[image]	创建时间	2024/09/03
[image]	**Description**	工具

1. ahmia.fi (https://ahmia.fi/) - 最著名的开源暗网搜索引擎之一的明网镜像；

1. onionengine.com (https://onionengine.com/)- 同上，只是该搜索引擎不那么热门；

1. darkhunt.net (https://darkhunt.net/)- 另一个在明网中搜索洋葱网站的工具，很有效，但有很多广告；

1. Thehiddenwiki.com (thehiddenwiki.com) - 古老的链接目录；

1. onionland.io (https://onionland.io/) - 在 Tor2Web 的支持下创建的搜索引擎。

当然您还可以谷歌“site:onion.ly”，也能找到不少 .onion 网站，但不建议在谷歌上搜索这类资源。
也同样不建议您使用明网工具搜索风险过高的暗网内容，原因一样。

更推荐本站曾经推荐过的暗网搜索引擎，通过在本站搜索 #tor 标签可找到它们。

[image]
[image]

开源剪贴板管理器

[image] 关键词	剪贴板 效率
[image] 创建时间	2024年9月6日
[image] **Description**	工具

PasteBar 是一款适用于 Mac 和 Windows 的开源剪贴板管理器，可轻松管理复制的内容。

主要功能包括无限的剪贴板历史记录、可搜索的复制历史记录、可自定义的保存片段、锁屏和密码保护 等等。

支持多种内容类型，如文本、图片、文件、链接和代码片段，并提供编程语言自动检测、语法高亮显示、笔记中的 Markdown 支持以及系统菜单中的即时粘贴功能。

 https://github.com/PasteBar/PasteBarApp

网站： https://www.pastebar.app/

[image]
[image]

开源剪贴板管理器

[image] 关键词	剪贴板 效率
[image] 创建时间	2024/09/06
[image] **Description**	工具

PasteBar 是一款适用于 Mac 和 Windows 的开源剪贴板管理器，可轻松管理复制的内容。

主要功能包括无限的剪贴板历史记录、可搜索的复制历史记录、可自定义的保存片段、锁屏和密码保护 等等。

支持多种内容类型，如文本、图片、文件、链接和代码片段，并提供编程语言自动检测、语法高亮显示、笔记中的 Markdown 支持以及系统菜单中的即时粘贴功能。

 https://github.com/PasteBar/PasteBarApp

网站： https://www.pastebar.app/

[image]
[image]

一系列免费的人工智能翻译器

[image] 关键词	效率
[image] 关联	[image]跨平台AI翻译 ；[image]一系列免费的人工智能翻译器 ；[image]实时语音翻译 ；[image]翻译视频
[image] 创建时间	2024年9月24日
[image] Description	工具

1. https://wordvice.ai/tools/translate

1. https://monica.im/ai-translate

1. https://quillbot.com/translate

1. https://sider.ai/en/products/chatgpt-ai-translator

1. https://www.deepl.com/ru/translator

1. https://openl.io/ru

1. https://felo.me/translate

1. https://www.smartcat.com/machine-translation/

1. https://textcortex.com/templates/pdf-document-translator

1. https://www.machinetranslation.com/ru

1. https://libretranslate.com/

1. https://customer.stepes.com/instant-translation-quote/

1. https://translate.hix.ai/

1. https://www.linguee.com/

1. https://papago.naver.com/

1. https://www.systransoft.com/lp/free-online-translation/

[image]
[image]

一系列免费的人工智能翻译器

[image] 关键词	效率
[image] 创建时间	2024/09/24
[image] **Description**	工具

1. https://wordvice.ai/tools/translate

1. https://monica.im/ai-translate

1. https://quillbot.com/translate

1. https://sider.ai/en/products/chatgpt-ai-translator

1. https://www.deepl.com/ru/translator

1. https://openl.io/ru

1. https://felo.me/translate

1. https://www.smartcat.com/machine-translation/

1. https://textcortex.com/templates/pdf-document-translator

1. https://www.machinetranslation.com/ru

1. https://libretranslate.com/

1. https://customer.stepes.com/instant-translation-quote/

1. https://translate.hix.ai/

1. https://www.linguee.com/

1. https://papago.naver.com/

1. https://www.systransoft.com/lp/free-online-translation/

[image]
[image]

去中心化的社交网络协议

[image] 关键词	去中心化 社交网络
[image] 创建时间	2024/10/08
[image] **Description**	工具

NOSTR 是一种去中心化的社交网络协议，使用公钥和私钥来提高安全性和隐私性。

与那些依赖单一服务器的集中式平台不同，它允许独立连接到世界各地的服务器（中继）。

主要特点：

- 应用区块链技术（BTC Lightning）；
- 用于数据存储的 IPFS；
- 公钥和私钥加密，让用户控制数据；
- 无中央服务器 - 完全去中心化的网络；

客户端：

浏览器
Snort

Yosup
Primal

iOS
Nos
Damus
Plebstr

安卓
Nostros
Amethyst

桌面
Gossip
more-speech
Lume

□ https://nostr.com/#resilient

[image]
[image]

去中心化的社交网络协议

[image] 关键词	去中心化 社交网络
[image] 关联	[image]免费的去中心化社交网络平台
[image] 创建时间	2024年10月8日
[image] **Description**	工具

NOSTR 是一种去中心化的社交网络协议，使用公钥和私钥来提高安全性和隐私性。

与那些依赖单一服务器的集中式平台不同，它允许独立连接到世界各地的服务器（中继）。

主要特点：

- 应用区块链技术（BTC Lightning）；
- 用于数据存储的 IPFS；
- 公钥和私钥加密，让用户控制数据；
- 无中央服务器 - 完全去中心化的网络；

客户端：

浏览器
Snort
Yosup
Primal

iOS
Nos
Damus
Plebstr

安卓
Nostros
Amethyst

桌面
Gossip
more-speech
Lume

 https://nostr.com/#resilient

[image]
[image]

完全Tor

[image] 关键词	tor
[image] 关联	[image]Tor工具系列
[image] 创建时间	2024年10月10日
[image] **Description**	工具

为探险家、密码朋克和好奇者准备的。更新版列表。

Tor信使

1. Tinfoil Chat https://github.com/maqp/tfc

1. Ricochet Refresh https://www.ricochetrefresh.net/

1. Briar https://briarproject.org

1. Speek https://speek.network/

1. cwtch.im https://cwtch.im/

1. Anonymous Messenger https://play.google.com/store/apps/details?id=com.dx.anonymousmessenger&hl=en_US&pli=1

1. Quiet https://github.com/TryQuiet/quiet

节点信息

1. TOR Node List https://www.dan.me.uk/tornodes

1. ExoneraTor https://metrics.torproject.org/exonerator.html

1. Onionite https://github.com/lukechilds/onionite

1. Tor Metrics https://metrics.torproject.org

1. Collector Tor https://collector.torproject.org/archive/relay-descriptors/microdescs/

节点使用

1. Tor Relay Availability Checker https://github.com/ValdikSS/tor-relay-scanner

1. noContactInfo Tor Exit Relay Excluder https://github.com/nusenu/noContactInfo_Exit_Excluder

1. Torspray https://github.com/gergelykalman/torspray

1. node-Tor https://github.com/Ayms/node-Tor

1. BridgeButtons https://github.com/kevinl95/BridgeButtons

网络爬虫

1. TorBot https://github.com/DedSecInside/TorBot

1. OnionBot https://github.com/Flobin/OnionBot

1. OnionIngestor https://github.com/danieleperera/OnionIngestor

1. Midnight Sea https://github.com/RicYaben/midnight_sea

1. VililantOnion https://github.com/andreyglauzer/VigilantOnion

1. OnionScan https://github.com/s-rah/onionscan

1. Fresh Onions TOR Hidden Service Crawler https://github.com/dirtyfilthy/freshonions-torscraper

1. Darkweb Crawler Project https://github.com/JarryShaw/darc

1. Tor Onion Site Scraper https://github.com/joelhagvall/tor-onion-site-scraper

1. TorCRAWL https://github.com/MikeMeliz/TorCrawl.py

搜索引擎（脚本）

1. Katana https://github.com/TebbaaX/Katana

1. OnionSearch https://github.com/megadose/OnionSearch

1. Darkdump https://github.com/josh0xA/darkdump

1. Darkus https://github.com/Lucksi/Darkus

搜索引擎（明网）

1. Ahima https://ahmia.fi/

1. OnionSearchEngine https://onionengine.com/

1. Darkhunt https://darkhunt.net

1. Onionland https://onionland.io/

搜索引擎（洋葱）

1. EXCAVATOR http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5f

1. Devil Search http://search65pq2x5oh4o4qlxk2zvoa5zhbfi6mx4br4oc33rpxuayauwsqd.on

1. TorDex http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onic

1. Torgle http://

iy3544gmoeclh5de6gez2256v6pjh4omhpqdh2wpeeppjtvqmjhkfwad.o
torgle/

1. Raklet http://
iwr4usy33opfclmbyemzbmnwwnmmqpqltezpac7fyqqkdv3mabtm6kq

1. Phobos http://
phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion

1. VormWeb http://
volkancfgpi4c7ghph6id2t7vcntenuly66qjt6oedwtjmyj4tkk5oqd.onion

1. Dig http://
digdig2nugjpszzmqe5ep2bk7lqfpdlyrkojsx2j6kzalnrqtwedr3id.onion/

1. Shoot http://
shootnnngg4akh7fkjmx5b5omsppt2zaefohzwnwryhy2c6mm3kbx6qd.

.ion网站的链接目录

1. UnderDir http://
underdiriled6lvdfgiw4e5urfofuslnz7ewictzf76h4qb73fxbsxad.onion/

1. Hidden Links http://
wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion

1. Dark Eye http://
darkeyepxw7cuu2cppnjlgqaav6j42gyt43clcn4vjjf7llfyly5cxid.onion/

1. Fresh Onions http://
freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad

1. Signpost http://signpostcjbbviqdhfbtocj6dthbd7cpvo3tpwrrfhkkk4fafjd53nyd.onion/

1. Deep Link http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.oni

1. Deep Links Dump http://deepqelxz6iddqi5obzla2bbwh5ssyqqobxin27uzkr624wtubhto3ad.onio

1. dark.fail https://dark.fail/

1. Tasty Onions http://22tojepqmpah32fkeuurutki7o5bmb45uhmgzdg4l2tk34fkdafgt

1. tor.taxi https://tor.taxi/

1. Dark Catalog http://catalogxlotjjnu6vyevngf675vu6beefzxw6gd6a3fwgmgznksrqmqd.onio latest.html

1. Onion link list http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/

1. Onion link online test http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/test.php

1. Deep Link Onion Directory http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.onio

1. Dark Web Pug's Ultimate Guide http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.oni

1. TOR Links List http://5n4qdkw2wavc55peppyrelmb2rgsx7ohcb2tkxhub2gyfurxulfyd

1. Hidden Wiki FRESH 2022 http://ieeppzy7cz254nz2iz7omykshnlap5ktjq3r7ujfpxagygaobpxfdbqd.onion

让流量通过 Tor

1. Orbot [Android] http://shootnnngg4akh7fkjmx5b5omsppt2zaefohzwnwryhy2c6mm3kbx6qd.

1. InviZible Pro [Android] https://apt.izzysoft.de/fdroid/index/apk/pan.alexander.tordnscrypt

1. Advanced Onion Router [Windows] https://sourceforge.net/projects/advtor/

1. Tallow [Windows] https://reqrypt.org/tallow.html

1. anon-service [*nix] https://github.com/bit4mind/anon-service

[image]
[image]

完全Tor

[image] 关键词	tor
[image] 创建时间	2024/10/10
[image] **Description**	工具

为探险家、密码朋克和好奇者准备的。更新版列表。

Tor信使

1. Tinfoil Chat https://github.com/maqp/tfc

1. Ricochet Refresh https://www.ricochetrefresh.net/

1. Briar https://briarproject.org

1. Speek https://speek.network/

1. cwtch.im https://cwtch.im/

1. Anonymous Messenger https://play.google.com/store/apps/details?id=com.dx.anonymousmessenger&hl=en_US&pli=1

1. Quiet https://github.com/TryQuiet/quiet

节点信息

1. TOR Node List https://www.dan.me.uk/tornodes

1. ExoneraTor https://metrics.torproject.org/exonerator.html

1. Onionite https://github.com/lukechilds/onionite

1. Tor Metrics https://metrics.torproject.org

1. Collector Tor https://collector.torproject.org/archive/relay-descriptors/microdescs/

节点使用

1. Tor Relay Availability Checker https://github.com/ValdikSS/tor-relay-scanner

1. noContactInfo Tor Exit Relay Excluder https://github.com/nusenu/noContactInfo_Exit_Excluder

1. Torspray https://github.com/gergelykalman/torspray

1. node-Tor https://github.com/Ayms/node-Tor

1. BridgeButtons https://github.com/kevinl95/BridgeButtons

网络爬虫

1. TorBot https://github.com/DedSecInside/TorBot

1. OnionBot https://github.com/Flobin/OnionBot

1. OnionIngestor https://github.com/danieleperera/OnionIngestor

1. Midnight Sea https://github.com/RicYaben/midnight_sea

1. VililantOnion https://github.com/andreyglauzer/VigilantOnion

1. OnionScan https://github.com/s-rah/onionscan

1. Fresh Onions TOR Hidden Service Crawler https://github.com/dirtyfilthy/freshonions-torscraper

1. Darkweb Crawler Project https://github.com/JarryShaw/darc

1. Tor Onion Site Scraper https://github.com/joelhagvall/tor-onion-site-scraper

1. TorCRAWL https://github.com/MikeMeliz/TorCrawl.py

搜索引擎（脚本）

1. Katana https://github.com/TebbaaX/Katana

1. OnionSearch https://github.com/megadose/OnionSearch

1. Darkdump https://github.com/josh0xA/darkdump

1. Darkus https://github.com/Lucksi/Darkus

搜索引擎（明网）

1. Ahima https://ahmia.fi/

1. OnionSearchEngine https://onionengine.com/

1. Darkhunt https://darkhunt.net

1. Onionland https://onionland.io/

搜索引擎（洋葱）

1. EXCAVATOR http://2fd6cemt4gmccflhm6imvdfvli3nf7zn6rfrwpsy7uhxrgbypvwf5f

1. Devil Search http://search65pq2x5oh4o4qlxk2zvoa5zhbfi6mx4br4oc33rpxuayauwsqd.on

1. TorDex http://tordexu73joywapk2txdr54jed4imqledpcvcuf75qsas2gwdgksvnyd.onio

1. Torgle http://

iy3544gmoeclh5de6gez2256v6pjh4omhpqdh2wpeeppjtvqmjhkfwad.o
torgle/

1. Raklet http://
iwr4usy33opfclmbyemzbmnwwnmmqpqltezpac7fyqqkdv3mabtm6kq

1. Phobos http://
phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion

1. VormWeb http://
volkancfgpi4c7ghph6id2t7vcntenuly66qjt6oedwtjmyj4tkk5oqd.onion

1. Dig http://
digdig2nugjpszzmqe5ep2bk7lqfpdlyrkojsx2j6kzalnrqtwedr3id.onion/

1. Shoot http://
shootnnngg4akh7fkjmx5b5omsppt2zaefohzwnwryhy2c6mm3kbx6qd.

.ion网站的链接目录

1. UnderDir http://
underdiriled6lvdfgiw4e5urfofuslnz7ewictzf76h4qb73fxbsxad.onion/

1. Hidden Links http://
wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion

1. Dark Eye http://
darkeyepxw7cuu2cppnjlgqaav6j42gyt43clcn4vjjf7llfyly5cxid.onion/

1. Fresh Onions http://
freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad

1. Signpost http://signpostcjbbviqdhfbtocj6dthbd7cpvo3tpwrrfhkkk4fafjd53nyd.onion/

1. Deep Link http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.onio

1. Deep Links Dump http://deepqelxz6iddqi5obzla2bbwh5ssyqqobxin27uzkr624wtubhto3ad.onio

1. dark.fail https://dark.fail/

1. Tasty Onions http://22tojepqmpah32fkeuurutki7o5bmb45uhmgzdg4l2tk34fkdafgt

1. tor.taxi https://tor.taxi/

1. Dark Catalog http://catalogxlotjjnu6vyevngf675vu6beefzxw6gd6a3fwgmgznksrqmqd.onio latest.html

1. Onion link list http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/

1. Onion link online test http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/test.php

1. Deep Link Onion Directory http://deepxfmkjlils3vd7bru5rrxy3x3lchjgmv3wsgycjfynktmuwgm64qd.onio

1. Dark Web Pug's Ultimate Guide http://jgwe5cjqdbyvudjqskaajbfibfewew4pndx52dye7ug3mt3jimmktkid.oni

1. TOR Links List http://5n4qdkw2wavc55peppyrelmb2rgsx7ohcb2tkxhub2gyfurxulfyd

1. Hidden Wiki FRESH 2022 http://ieeppzy7cz254nz2iz7omykshnlap5ktjq3r7ujfpxagygaobpxfdbqd.onion

让流量通过 Tor

1. Orbot [Android] http://shootnnngg4akh7fkjmx5b5omsppt2zaefohzwnwryhy2c6mm3kbx6qd.

1. InviZible Pro [Android] https://apt.izzysoft.de/fdroid/index/apk/pan.alexander.tordnscrypt

1. Advanced Onion Router [Windows] https://sourceforge.net/projects/advtor/

1. Tallow [Windows] https://reqrypt.org/tallow.html

1. anon-service [*nix] https://github.com/bit4mind/anon-service

[image]
[image]

安全存储照片和视频

[image]	关键词	传输安全 加密 反侦察
[image]	创建时间	2024年10月14日
[image]	**Description**	工具

Photok 是一款免费的开源应用程序，旨在安全地加密和存储您设备上的照片和视频，防止未经授权的访问。

Photok 使用 AES-256 标准和 bcrypt 等先进的加密技术，确保您的媒体文件保持私密性并受到保护。

无广告，提供多种功能，包括导入和导出照片和视频、更改密码、创建和恢复备份、通过 Photok 共享文件、隐藏应用程序图标和访问恢复菜单。

 https://github.com/leonlatsch/Photok

F-droid: https://github.com/leonlatsch/Photok

[image]
[image]

安全存储照片和视频

[image] 关键词	传输安全 加密 反侦察
[image] 创建时间	2024/10/14
[image] **Description**	工具

Photok 是一款免费的开源应用程序，旨在安全地加密和存储您设备上的照片和视频，防止未经授权的访问。

Photok 使用 AES-256 标准和 bcrypt 等先进的加密技术，确保您的媒体文件保持私密性并受到保护。

无广告，提供多种功能，包括导入和导出照片和视频、更改密码、创建和恢复备份、通过 Photok 共享文件、隐藏应用程序图标和访问恢复菜单。

 https://github.com/leonlatsch/Photok

F-droid: https://github.com/leonlatsch/Photok

[image]
[image]

去除图像中的水印和其他元素

[image]	关键词	元数据 数字足迹 自助
[image]	创建时间	2024年10月22日
[image]	**Description**	工具

1. cleanup.pictures (https://cleanup.pictures/) - 用于删除照片中的各种对象：人物、文本和其他任何指定的对象。

1. TouchRemove (https://play.google.com/store/apps/details?id=com.genewarrior.touchremove2&hl=en_US&gl=US) - Android 上的类似应用程序，不仅可以删除，还可以移动照片上的对象。

1. Downloader.la (downloader.la) - 从 Getty Images、Adobe Stock 和 DepositPhotos 下载无水印图片。

1. Watermark Remover (https://www.watermarkremover.io) - 几秒钟去除照片上的所有水印。

1. Hama (https://www.hama.app/en) - 同样使用神经网络去除照片中的对象物体。

1. ANYMP4 (https://www.anymp4.com/watermark-remover-online/) - 另一款使用人工智能的免费水印去除服务。

1. iMyFone MarkGo (https://filme.imyfone.com/watermark-

remover/) - 可去除图片和视频中的水印。

1. Aiseesoft Free Watermark Remover (https://www.aiseesoft.com/watermark-remover-online/) - 免费在线工具，使用 AI。

1. Watermarkremover (https://www.watermarkremover.io/) - 另一款免费在线去水印工具。

1. Inpaint (https://theinpaint.com/) - 免费工具，有桌面版和在线版。

1. Fotophire Photo Eraser (https://photo.wondershare.com/photo-eraser.html) - 桌面版，简单但功能强大的照片编辑器。有试用版。

1. Fotor (https://www.fotor.com/features/remove-watermark-from-photo/) - 也是在线工具。

1. https://acetone.ai/

1. https://snapedit.app/ru/remove-object

1. https://snapedit.app/ru

1. https://picwish.com/remove-unwanted-object

1. https://firefly.adobe.com

1. https://www.artguru.ai/ru/remove-object-from-photo/

1. https://anieraser.media.io/app/

1. https://clearoff.imagewith.ai/

1. https://www.photoroom.com/tools/remove-object-from-photo

1. https://www.ifoto.ai/watermark-remover

1. https://www.avaide.com/watermark-remover/

1. https://remaker.ai/features/ai-remove-object/

1. https://www.x-design.com/object-remover

1. https://www.zmo.ai/ai-photo-editor/remove-watermark-from-photo/

1. https://myedit.online/en/photo-editor/object-removal

[image]
[image]

去除图像中的水印和其他元素

[image] 关键词	元数据 数字足迹 自助
[image] 创建时间	2024/10/22
[image] **Description**	工具

1. cleanup.pictures (https://cleanup.pictures/) - 用于删除照片中的各种对象：人物、文本和其他任何指定的对象。

1. TouchRemove (https://play.google.com/store/apps/details?id=com.genewarrior.touchremove2&hl=en_US&gl=US) - Android 上的类似应用程序，不仅可以删除，还可以移动照片上的对象。

1. Downloader.la (downloader.la) - 从 Getty Images、Adobe Stock 和 DepositPhotos 下载无水印图片。

1. Watermark Remover (https://www.watermarkremover.io) - 几秒钟去除照片上的所有水印。

1. Hama (https://www.hama.app/en) - 同样使用神经网络去除照片中的对象物体。

1. ANYMP4 (https://www.anymp4.com/watermark-remover-online/) - 另一款使用人工智能的免费水印去除服务。

1. iMyFone MarkGo (https://filme.imyfone.com/watermark-

remover/) - 可去除图片和视频中的水印。

1. Aiseesoft Free Watermark Remover (https://www.aiseesoft.com/watermark-remover-online/) - 免费在线工具，使用 AI。

1. Watermarkremover (https://www.watermarkremover.io/) - 另一款免费在线去水印工具。

1. Inpaint (https://theinpaint.com/) - 免费工具，有桌面版和在线版。

1. Fotophire Photo Eraser (https://photo.wondershare.com/photo-eraser.html) - 桌面版，简单但功能强大的照片编辑器。有试用版。

1. Fotor (https://www.fotor.com/features/remove-watermark-from-photo/) - 也是在线工具。

1. https://acetone.ai/

1. https://snapedit.app/ru/remove-object

1. https://snapedit.app/ru

1. https://picwish.com/remove-unwanted-object

1. https://firefly.adobe.com

1. https://www.artguru.ai/ru/remove-object-from-photo/

1. https://anieraser.media.io/app/

1. https://clearoff.imagewith.ai/

1. https://www.photoroom.com/tools/remove-object-from-photo

1. https://www.ifoto.ai/watermark-remover

1. https://www.avaide.com/watermark-remover/

1. https://remaker.ai/features/ai-remove-object/

1. https://www.x-design.com/object-remover

1. https://www.zmo.ai/ai-photo-editor/remove-watermark-from-photo/

1. https://myedit.online/en/photo-editor/object-removal

[image]
[image]

备份和恢复已删除的文件

[image] 关键词	数据丢失
[image] 关联	[image]加密、生成校验和销毁文件 ；[image]备份和恢复已删除的文件
[image] 创建时间	2024年11月13日
[image] **Description**	工具

RescueZilla 是一个开源项目，用于备份和恢复已删除的文件。

- 无需安装，可通过 U 盘或 CD 光盘运行；
- 可保存和还原 Windows、MacOS 和 Linux 设备；
- 支持 VirtualBox、VMWare、Qemu 等镜像；
- 可恢复已删除的照片、文档和其他文件；
- 允许复制任何磁盘，包括系统磁盘；
- 内置浏览器；

它是 Clonezilla 的一个变体，具有方便的图形界面，多语种以及其他功能。

https://rescuezilla.com/

[image]
[image]

备份和恢复已删除的文件

[image]	关键词	数据丢失
[image]	创建时间	2024/11/13
[image]	**Description**	工具

RescueZilla 是一个开源项目，用于备份和恢复已删除的文件。

- 无需安装，可通过 U 盘或 CD 光盘运行；
- 可保存和还原 Windows、MacOS 和 Linux 设备；
- 支持 VirtualBox、VMWare、Qemu 等镜像；
- 可恢复已删除的照片、文档和其他文件；
- 允许复制任何磁盘，包括系统磁盘；
- 内置浏览器；

它是 Clonezilla 的一个变体，具有方便的图形界面，多语种以及其他功能。

 https://rescuezilla.com/

[image]
[image]

伪造手机位置

[image]	关键词	免追踪 定位 自助
[image]	创建时间	2024年11月14日
[image]	**Description**	工具

FakeTraveler 是一款用于伪造手机位置的安卓应用程序，可用于隐私保护或应用程序测试。

它允许您在地图上选择一个位置或输入特定的经纬度坐标，然后应用这些设置来伪造设备的位置。

其他功能还包括在特定时间段内设置虚假位置。

要使用 FakeTraveler，需要在设备上启用开发者设置，并在设置中选择 FakeTraveler 作为位置欺骗应用程序。

 https://github.com/mcastillof/FakeTraveler

 F-droid: https://f-droid.org/packages/cl.coders.faketraveler/

[image]
[image]

使用容器隔离应用程序和虚拟机

[image] 关键词	tor 沙箱 虚拟机 预防性
[image] 创建时间	2024年11月14日
[image] **Description**	工具

QuBSD 是一种 BSD 系统，它使用 jails 和 bhyve 等 FreeBSD 工具模仿 Qubes Linux 的容器化。

该系统基于 ZFS 文件系统，使用容器隔离应用程序和虚拟机。

此外，还通过独立的虚拟机隔离 PCI、网络和 USB 设备，以提高安全性。

该项目还计划进行进一步开发，如 Tor 网关实施、GUI隔离和加密 Jails。

 https://github.com/BawdyAnarchist/quBSD

[image]
[image]

使用容器隔离应用程序和虚拟机

[image] 关键词	tor 沙箱 虚拟机 预防性
[image] 创建时间	2024/11/14
[image] **Description**	工具

QuBSD 是一种 BSD 系统，它使用 jails 和 bhyve 等 FreeBSD 工具模仿 Qubes Linux 的容器化。

该系统基于 ZFS 文件系统，使用容器隔离应用程序和虚拟机。

此外，还通过独立的虚拟机隔离 PCI、网络和 USB 设备，以提高安全性。

该项目还计划进行进一步开发，如 Tor 网关实施、GUI隔离和加密 Jails。

 https://github.com/BawdyAnarchist/quBSD

[image]
[image]

伪造手机位置

[image] 关键词	免追踪 定位 自助
[image] 创建时间	2024/11/14
[image] **Description**	工具

FakeTraveler 是一款用于伪造手机位置的安卓应用程序，可用于隐私保护或应用程序测试。

它允许您在地图上选择一个位置或输入特定的经纬度坐标，然后应用这些设置来伪造设备的位置。

其他功能还包括在特定时间段内设置虚假位置。

要使用 FakeTraveler，需要在设备上启用开发者设置，并在设置中选择 FakeTraveler 作为位置欺骗应用程序。

 https://github.com/mcastillof/FakeTraveler

 F-droid: https://f-droid.org/packages/cl.coders.faketraveler/

[image]
[image]

一些工具都可用来恢复已删除的文件

[image]	关键词	反侦察 对抗性思考方式 数据丢失 自助
[image]	创建时间	2024/11/15
[image]	**Description**	工具

1. Recuva (https://www.ccleaner.com/zh-cn/recuva)- 来自著名的CCleaner的免费软件，用于恢复误删的文件。

1. Puran File Recovery (http://www.puransoftware.com/File-Recovery-Download.html) - 是一款简约的软件，具有多种扫描模式，支持50种文件格式；

1. Glary Undelete(https://www.glarysoft.com/file-recovery-free/) - 另一款不错的解决方案，支持恢复被压缩的、粉碎的和加密的文件；

1. TestDisk (https://github.com/cgsecurity/testdisk) - 是一款功能强大的免费程序，可恢复在各种情况下删除的数据：由于恶意软件、错误、系统崩溃或意外删除整个磁盘分区；

1. RescueZilla (https://rescuezilla.com/) - 是一个开源项目，用于备份和恢复已删除的文件；

1. Disk Drill (https://github.com/deogroupvinkars1988/Disk-Drill) - 可免费恢复高达 500 MB 的丢失文件：各种格式的照

片、图像、视频和音乐文件。

1. Restoration (https://restoration.informer.com/3.2/) - 老式版本，适用于文件系统：FAT12、FAT16、FAT32 和 NTFS。能够恢复通过回收站或 “Shift + Del ”快捷方式删除的文件和文件夹。

[image]
[image]

开源跨浏览器管理器

[image] 关键词	效率 浏览器
[image] 创建时间	2024年11月15日
[image] **Description**	工具

Unsearch 是一款开源的跨浏览器管理器，用于在一个集中位置同步和管理多个浏览器的书签和浏览历史记录。

它旨在解决主流浏览器提供的同步限制问题，这些限制往往会将用户锁定在某些生态系统中，并导致隐私风险。

Unsearch 提供的功能包括高级搜索过滤器、数据保留自定义规则和端对端加密，以保护隐私和进行控制。

开源技术的使用使 Unsearch 保持透明和安全，不受企业利益的影响。

 https://github.com/unsearchapp/unsearch

 网站：https://unsearch.app/

[image]
[image]

一些工具都可用来恢复已删除的文件

[image]	关键词	反侦察 对抗性思考方式 数据丢失 自助
[image]	创建时间	2024年11月15日
[image]	Description	工具

1. Recuva (https://www.ccleaner.com/zh-cn/recuva)- 来自著名的CCleaner的免费软件，用于恢复误删的文件。

1. Puran File Recovery (http://www.puransoftware.com/File-Recovery-Download.html) - 是一款简约的软件，具有多种扫描模式，支持50种文件格式；

1. Glary Undelete(https://www.glarysoft.com/file-recovery-free/) - 另一款不错的解决方案，支持恢复被压缩的、粉碎的和加密的文件；

1. TestDisk (https://github.com/cgsecurity/testdisk) - 是一款功能强大的免费程序，可恢复在各种情况下删除的数据：由于恶意软件、错误、系统崩溃或意外删除整个磁盘分区；

1. RescueZilla (https://rescuezilla.com/) - 是一个开源项目，用于备份和恢复已删除的文件；

1. Disk Drill (https://github.com/deogroupvinkars1988/Disk-Drill) - 可免费恢复高达 500 MB 的丢失文件：各种格式的照

片、图像、视频和音乐文件。

1. Restoration (https://restoration.informer.com/3.2/) - 老式版本，适用于文件系统：FAT12、FAT16、FAT32 和 NTFS。能够恢复通过回收站或 “Shift + Del ”快捷方式删除的文件和文件夹。

[image]
[image]

开源跨浏览器管理器

[image]	关键词	效率 浏览器
[image]	创建时间	2024/11/15
[image]	**Description**	工具

Unsearch 是一款开源的跨浏览器管理器，用于在一个集中位置同步和管理多个浏览器的书签和浏览历史记录。

它旨在解决主流浏览器提供的同步限制问题，这些限制往往会将用户锁定在某些生态系统中，并导致隐私风险。

Unsearch 提供的功能包括高级搜索过滤器、数据保留自定义规则和端对端加密，以保护隐私和进行控制。

开源技术的使用使 Unsearch 保持透明和安全，不受企业利益的影响。

 https://github.com/unsearchapp/unsearch

 网站：https://unsearch.app/

[image]
[image]

安卓的网状网络解决方案

[image] 关键词	安卓 离线
[image] 关联	[image]离线安全存储 - 完全本地无需服务器 ；[image]离线安全传输 ；[image]带有频道功能的离线P2P安全通信 ；[image]开源点对点社交网络 ；[image]断网后通信：把智能手机变成“对讲机” ；[image]网状网络通信，支持 LoRa 设备
[image] 创建时间	2024年11月19日
[image] **Description**	工具

Meshrabiya 是一种适用于安卓的网状网络解决方案。适用于多个 Android 设备需要相互通信且 WiFi 接入点不可用的情况。

完全开源，没有任何专有依赖项，独立于 GooglePlay 服务。

Meshrabiya 还能创建用于数据传输的套接字。还可以与其他网络库（例如 OkHttp）一起使用，以便轻松地通过虚拟网格发送/接收数据。

另为开发人员提供了测试应用和说明，包括创建虚拟节点和配置连接。

 https://github.com/UstadMobile/Meshrabiya

[image]
[image]

安卓的网状网络解决方案

[image]	关键词	安卓 离线
[image]	创建时间	2024/11/19
[image]	**Description**	工具

Meshrabiya 是一种适用于安卓的网状网络解决方案。适用于多个 Android 设备需要相互通信且 WiFi 接入点不可用的情况。

完全开源，没有任何专有依赖项，独立于 GooglePlay 服务。

Meshrabiya 还能创建用于数据传输的套接字。还可以与其他网络库（例如 OkHttp）一起使用，以便轻松地通过虚拟网格发送/接收数据。

另为开发人员提供了测试应用和说明，包括创建虚拟节点和配置连接。

 https://github.com/UstadMobile/Meshrabiya

[image]
[image]

开源加密工具

[image]	关键词	加密 文件处理 查询整理 预防性
[image]	创建时间	2024/11/20
[image]	**Description**	工具

VeraCrypt 是一款开源加密工具。它是 TruCrypt 的分叉，已修复漏洞。

特点：

- 创建存储重要文件和文件夹的加密软件容器。
- 加密光盘、其逻辑分区和闪存盘。

加密U盘

点击 “创建加密卷”→选择 “加密非系统分区”→“下一步”并允许安装驱动程序→选择 “VeraCrypt 常规加密卷”，点击 “下一步”。

选择加密卷位置并勾选闪存盘，点击 “确定”→选择 “创建并格式化加密卷”→“下一步”→选择加密算法→“下一步”→设置加密卷密码并格式化闪存盘。

 https://www.veracrypt.fr/en/Downloads.html

[image]
[image]

开源加密工具

[image] 关键词	加密 文件处理 查询整理 预防性
[image] 创建时间	2024年11月20日
[image] **Description**	工具

VeraCrypt 是一款开源加密工具。它是 TruCrypt 的分叉，已修复漏洞。

特点：

- 创建存储重要文件和文件夹的加密软件容器。
- 加密光盘、其逻辑分区和闪存盘。

加密U盘

点击“创建加密卷”→选择“加密非系统分区”→“下一步”并允许安装驱动程序→选择“VeraCrypt 常规加密卷”，点击“下一步”。

选择加密卷位置并勾选闪存盘，点击“确定”→选择“创建并格式化加密卷”→“下一步”→选择加密算法→“下一步”→设置加密卷密码并格式化闪存盘。

 https://www.veracrypt.fr/en/Downloads.html

[image]
[image]

匿名托管服务

[image]	关键词	匿名托管 反封锁 自助
[image]	创建时间	2024/11/21
[image]	**Description**	工具

匿名托管服务：无需 KYC 的服务器和/或域名。

您懂的……

Njalla：https://njal.la/
NiceVPS：https://nicevps.net/
AnyCOLO：https://anycolo.net/
FlokiNET：https://flokinet.is/
IncogNET：https://incognet.io/
Hostiko：https://hostiko.com.ua/en
CryptoHO.ST：https://cryptoho.st/
1984 Hosting：https://1984.hosting/
OrangeWebsite：https://www.orangewebsite.com
Greenhost：https://greenhost.net/

[image]
[image]

匿名托管服务VPS

[image] 关键词	匿名托管 反封锁 自助
[image] 创建时间	2024年11月21日
[image] **Description**	工具

匿名托管服务：无需 KYC 的服务器和/或域名。

您懂的……

Njalla：https://njal.la/
NiceVPS：https://nicevps.net/
AnyCOLO：https://anycolo.net/
FlokiNET：https://flokinet.is/
IncogNET：https://incognet.io/
Hostiko：https://hostiko.com.ua/en
CryptoHO.ST：https://cryptoho.st/
1984 Hosting：https://1984.hosting/
OrangeWebsite：https://www.orangewebsite.com
Greenhost：https://greenhost.net/

[image]
[image]

轻量级的高效隐写工具

[image]	关键词	隐写术
[image]	创建时间	2024/11/25
[image]	**Description**	工具

SteganoPass 是一款轻量级的高效隐写工具，用于将加密的秘密消息隐藏在图像中，支持 JPG、BMP、PNG、TGA 和 PSD 格式。

软件界面很简单，可以轻松上传图片，使用自定义密钥隐藏和提取信息。

 https://github.com/psdoood/SteganoPass

[image]
[image]

轻量级的高效隐写工具

[image] 关键词	隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2024年11月25日
[image] **Description**	工具

SteganoPass 是一款轻量级的高效隐写工具，用于将加密的秘密消息隐藏在图像中，支持 JPG、BMP、PNG、TGA 和 PSD 格式。

软件界面很简单，可以轻松上传图片，使用自定义密钥隐藏和提取信息。

 https://github.com/psdoood/SteganoPass

[image]
[image]

备份/恢复工具

[image]	关键词	加密 备份 数据丢失
[image]	创建时间	2024/12/03
[image]	**Description**	工具

Kopia 是一款备份/恢复工具，开源，具有E2E加密和重复数据删除等功能。

与传统工具不同，它允许您备份单个文件和目录，而不是创建完整的系统镜像。

它提供图形用户界面和命令行两个版本，专业人士和普通用户都适用。

 https://github.com/kopia/kopia

[image]
[image]

备份/恢复工具

[image] 关键词	加密 备份 数据丢失
[image] 创建时间	2024年12月3日
[image] **Description**	工具

Kopia 是一款备份/恢复工具，开源，具有E2E加密和重复数据删除等功能。

与传统工具不同，它允许您备份单个文件和目录，而不是创建完整的系统镜像。

它提供图形用户界面和命令行两个版本，专业人士和普通用户都适用。

 https://github.com/kopia/kopia

[image]
[image]

给Tor网络研究人员的小工具

[image] 关键词	tor
[image] 创建时间	2024年12月10日
[image] **Description**	工具

1. Torboost (https://github.com/tasooshi/torboost) - 用于从洋葱服务下载大文件以作进一步分析的工具；

1. Tor-util (https://github.com/GIJack/tor-util) - 网络API实用程序，如请求新IP，或生成API密码；

1. Carml (https://github.com/meejah/carml) - 是一个命令行工具，用于启动Tor和进一步管理；

1. NGTOR (https://github.com/theborakompanioni/ngtor) - 用于通过Tor传输隧道流量、处理静态数据等的实用工具；

1. torget (https://github.com/mtrojnar/torget) - 另一个下载大文件的工具，速度更快；

1. Torutils (https://github.com/toralf/torutils) - 用于保护Tor节点免受DDoS攻击的脚本集.

[image]
[image]

给Tor网络研究人员的小工具

[image] 关键词	tor
[image] 创建时间	2024/12/10
[image] Description	工具

1. Torboost (https://github.com/tasooshi/torboost) - 用于从洋葱服务下载大文件以作进一步分析的工具；

1. Tor-util (https://github.com/GIJack/tor-util) - 网络API实用程序，如请求新IP，或生成API密码；

1. Carml (https://github.com/meejah/carml) - 是一个命令行工具，用于启动Tor和进一步管理；

1. NGTOR (https://github.com/theborakompanioni/ngtor) - 用于通过Tor传输隧道流量、处理静态数据等的实用工具；

1. torget (https://github.com/mtrojnar/torget) - 另一个下载大文件的工具，速度更快；

1. Torutils (https://github.com/toralf/torutils) - 用于保护Tor节点免受DDoS攻击的脚本集.

[image]
[image]

聊天IMs

[image] 关键词	IMs tor 传输安全 加密
[image] 创建时间	2024/12/17
[image] Description	工具

1. Mumble (https://www.mumble.info/downloads/) 一款免费开源的跨平台 VoIP 信使；

1. Quiet (https://github.com/TryQuiet/quiet) Slack、Discord 和 Element 等团队聊天应用程序的免费替代品，所有数据都通过 Tor；

1. Vencord (https://github.com/Vendicated/Vencord) - 一个不错的 Discord 替代客户端，隐私友好，很多插件；

1. Revolt.Chat (https://revolt.chat/) 开源的 Discord 类似软件，具有高级功能，在欧洲，隐私友好，自定义机器人和客户端很容易；

1. Teamspeak (https://www.teamspeak.com/en/) - 军事级的安全性，跨平台，高语音质量，插件众多；

1. Guilded (https://www.teamspeak.com/en/) - 另一个面向游戏玩家的信使。

[image]
[image]

安全IMs

[image] 关键词	IMs tor 传输安全 加密
[image] 关联	[image]一系列安全的即时通信软件和服务 ；离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线P2P安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；网状网络通信，支持LoRa 设备
[image] 创建时间	2024年12月17日
[image] **Description**	工具

1. Mumble (https://www.mumble.info/downloads/) 一款免费开源的跨平台 VoIP 信使；

1. Quiet (https://github.com/TryQuiet/quiet) Slack、Discord 和 Element 等团队聊天应用程序的免费替代品，所有数据都通过 Tor；

1. Vencord (https://github.com/Vendicated/Vencord) - 一个不错的 Discord 替代客户端，隐私友好，很多插件；

1. Revolt.Chat (https://revolt.chat/) 开源的 Discord 类似软件，具有高级功能，在欧洲，隐私友好，自定义机器人和客户端很容易；

1. Teamspeak (https://www.teamspeak.com/en/) - 军事级的安全性，跨平台，高语音质量，插件众多；

1. Guilded (https://www.teamspeak.com/en/) - 另一个面向游戏玩家的信使。

[image]
[image]

安卓文件管理和清理工具

[image] 关键词	反侦察 安卓 查询整理
[image] 创建时间	2025年1月4日
[image] **Description**	工具

SD Maid 2/SE 是一款面向安卓用户的高级文件管理器和清理工具。

- 卸载应用程序后进行清理；
- 删除不必要的文件和隐藏的缓存；
- 智能搜索设备；
- 高效的存储管理；
- 搜索重复的数据；
- 可选自动执行繁琐操作；
- 支持 Root 和 Shizuku；

 https://f-droid.org/ru/packages/eu.darken.sdmse/

[image]
[image]

安卓文件管理和清理工具

[image]	关键词	反侦察 安卓 查询整理
[image]	创建时间	2025/01/04
[image]	**Description**	工具

SD Maid 2/SE 是一款面向安卓用户的高级文件管理器和清理工具。

- 卸载应用程序后进行清理；
- 删除不必要的文件和隐藏的缓存；
- 智能搜索设备；
- 高效的存储管理；
- 搜索重复的数据；
- 可选自动执行繁琐操作；
- 支持 Root 和 Shizuku；

 https://f-droid.org/ru/packages/eu.darken.sdmse/

[image]
[image]

来自 GitHub 的AI工具目录

[image]	关键词	AI
[image]	创建时间	2025/01/05
[image]	**Description**	工具

以下是排名前 10 位的目录，这些目录按内部分类，包含数千种不同的人工智能产品，更容易找到适合您应用的神经网络。

1. https://github.com/ai-collection/ai-collection https://github.com/ghimiresunil/Top-AI-Tools

1. https://github.com/mahseema/awesome-ai-toolshttps://github.com/re50urces/Awesome-AI 5. https://github.com/yousefebrahimi0/1000-AI-collection-tools 6.

1. https://github.com/cloudcommunity/AI-Tools

1. https://github.com/amusi/awesome-ai-awesomeness

1. https://github.com/hades217/awesome-ai

1. https://github.com/mehmetkahya0/AI-Catalog

1. https://github.com/owainlewis/awesome-artificial-intelligence

当然还有网站（以前说过）：
https://www.aixploria.com/en/https://ailibri.com/en/productivity/https://theresanaiforthat.com/

[image]
[image]

来自 GitHub 的AI工具目录

[image] 关键词	AI
[image] 创建时间	2025年1月5日
[image] **Description**	工具

以下是排名前 10 位的目录，这些目录按内部分类，包含数千种不同的人工智能产品，更容易找到适合您应用的神经网络。

1. https://github.com/ai-collection/ai-collection https://github.com/ghimiresunil/Top-AI-Tools

1. https://github.com/mahseema/awesome-ai-toolshttps://github.com/re50urces/Awesome-AI 5. https://github.com/yousefebrahimi0/1000-AI-collection-tools 6.

1. https://github.com/cloudcommunity/AI-Tools

1. https://github.com/amusi/awesome-ai-awesomeness

1. https://github.com/hades217/awesome-ai

1. https://github.com/mehmetkahya0/AI-Catalog

1. https://github.com/owainlewis/awesome-artificial-intelligence

当然还有网站（以前说过）：
https://www.aixploria.com/en/https://ailibri.com/en/productivity/https://theresanaiforthat.com/

[image]
[image]

定期清理硬盘

[image] 关键词	反侦察 彻底擦除 自主 预防性
[image] 创建时间	2025/03/10
[image] **Description**	工具

如您所知，通过回收站进行的定期删除，或者使用Shift键进行删除，并不足以完全删除磁盘上的数据。通过这种方法删除的文件很容易恢复。

以下是一些旨在彻底删除数据的工具。

1. Darik's Boot and Nuke (https://dban.org/) - 开源的数据清除程序，可以用它来彻底清除硬盘上的所有文件，有免费试用。

1. File Shredder (https://www.fileshredder.org/) -是一款免费程序，可从硬盘驱动器和各种移动存储介质中不可逆地清除文件夹和文件。

1. File Nuke (https://sourceforge.net/projects/filenuke/) - 是一款便携式开源文件粉碎器，适用于Windows用户。

1. ShredOS (https://github.com/PartialVolume/shredos.x86_64) - 是一款小型 Linux 发行版，带有一个 “nwipe ”实用程序，可从硬盘中无痕迹地清除数据。

1. Disk Wipe (https://www.diskwipe.org/ - 是另一款不错的开源

无痕擦除工具。

[image]
[image]

定性清理硬盘

[image] 关键词	反侦察 彻底擦除 自主 预防性
[image] 创建时间	2025年3月10日
[image] **Description**	工具

如您所知，通过回收站进行的定期删除，或者使用Shift键进行删除，并不足以完全删除磁盘上的数据。通过这种方法删除的文件很容易恢复。

以下是一些旨在彻底删除数据的工具。

1.Darik's Boot and Nuke (https://dban.org/) - 开源的数据清除程序，可以用它来彻底清除硬盘上的所有文件，有免费试用。

1. File Shredder (https://www.fileshredder.org/) -是一款免费程序，可从硬盘驱动器和各种移动存储介质中不可逆地清除文件夹和文件。

1. File Nuke (https://sourceforge.net/projects/filenuke/) - 是一款便携式开源文件粉碎器，适用于Windows用户。

1. ShredOS (https://github.com/PartialVolume/shredos.x86_64) - 是一款小型 Linux 发行版，带有一个 “nwipe ”实用程序，可从硬盘中无痕迹地清除数据。

1. Disk Wipe (https://www.diskwipe.org/ - 是另一款不错的开源

无痕擦除工具。

[image]
[image]

使用临时网络命名空间通过 VPN 运行应用程序

[image] 关键词		代理
[image] 创建时间		2025年3月12日
[image] **Description**		工具

vopono 是一款允许你使用临时网络命名空间通过 VPN 运行应用程序的工具，它提供了在不同 VPN 上同时运行多个应用程序的能力，同时保持主连接。

它支持 Wireguard 和 OpenVPN（带紧急终止开关），以及包括 Mullvad 和 NordVPN 在内的多个提供商，并提供使用自定义配置的功能。

该工具可管理多达255个网络命名空间，并允许将设置保存到配置文件中。

 https://github.com/jamesmcm/vopono

[image]
[image]

使用临时网络命名空间通过 VPN 运行应用程序

[image] 关键词	代理
[image] 创建时间	2025/03/12
[image] **Description**	工具

vopono 是一款允许你使用临时网络命名空间通过 VPN 运行应用程序的工具，它提供了在不同 VPN 上同时运行多个应用程序的能力，同时保持主连接。

它支持 Wireguard 和 OpenVPN（带紧急终止开关），以及包括 Mullvad 和 NordVPN 在内的多个提供商，并提供使用自定义配置的功能。

该工具可管理多达255个网络命名空间，并允许将设置保存到配置文件中。

□ https://github.com/jamesmcm/vopono

[image]
[image]

在不同操作系统之间传输文件

[image] 关键词	IMs 传输安全 加密
[image] 关联	[image]在不安全渠道上尽可能安全地共享秘密 ；[image]安全的秘密共享 ；[image]点对点文件传输 ；[image]一些私密安全的文件传输解决方案 ；[image]在任何聊天工具中发送算对端加密信息 ；[image]安全共享 ；
[image] 创建时间	2025年3月13日
[image] **Description**	工具

1. Flying Carpet (https://github.com/spieglt/FlyingCarpet) - 通过 Wi-Fi 在 Android、iOS、Linux、macOS 和 Windows 之间传输文件；

1. RetroShare (https://retroshare.cc/) - 免费的跨平台软件，可通过加密的 F2F/P2P 网络无服务器交换电子邮件、即时消息和文件；

1. SendAnywhere (https://send-anywhere.com/)- 与 AirDrop 类似，支持多种操作系统；

1. Resilio Sync (https://www.resilio.com/sync/) - 通过 BitTorrent 在任意设备之间进行文件同步和备份的服务；

1. Syncthing (https://syncthing.net/) - 另一种使用 TLS PFS 加密的文件同步服务。

[image]
[image]

在不同操作系统之间传输文件

[image]	关键词	IMs 传输安全 加密
[image]	创建时间	2025/03/13
[image]	**Description**	工具

1. Flying Carpet (https://github.com/spieglt/FlyingCarpet) - 通过 Wi-Fi 在 Android、iOS、Linux、macOS 和 Windows 之间传输文件；

1. RetroShare (https://retroshare.cc/) - 免费的跨平台软件，可通过加密的 F2F/P2P 网络无服务器交换电子邮件、即时消息和文件；

1. SendAnywhere (https://send-anywhere.com/)- 与 AirDrop 类似，支持多种操作系统；

1. Resilio Sync (https://www.resilio.com/sync/) - 通过 BitTorrent 在任意设备之间进行文件同步和备份的服务；

1. Syncthing (https://syncthing.net/) - 另一种使用 TLS PFS 加密的文件同步服务。

[image]
[image]

将操作系统映像写入USB

[image] 关键词	安卓
[image] 创建时间	2025年3月17日
[image] **Description**	工具

EtchDroid 是一款开源 Android 应用程序，用于将操作系统映像写入USB记忆棒，包括 GNU/Linux 映像。

 https://github.com/etchdroid/etchdroid

[image]
[image]

将操作系统映像写入USB

[image] 关键词	安卓
[image] 创建时间	2025/03/17
[image] **Description**	工具

EtchDroid 是一款开源 Android 应用程序，用于将操作系统映像写入USB记忆棒，包括 GNU/Linux 映像。

 https://github.com/etchdroid/etchdroid

[image]
[image]

加密、生成校验和销毁文件

[image]	关键词	加密 查询整理 身份验证
[image]	创建时间	2025/03/18
[image]	**Description**	工具

Picocrypt 是一款简单实用的工具，可用于加密文件、生成校验和销毁文件等。

Picocrypt 使用安全的 XChaCha20流密码和 Argon2加密算法来提供高级保护。

▫Picocrypt 很小巧，仅 3MB

▫Picocrypt 便携式（无需安装），不需要管理员/root 权限。

▫Picocrypt 提供一个安全密码生成器，你可以用它来创建加密安全密码。

▫Picocrypt 支持使用密钥文件作为额外（或唯一）的身份验证形式。

以及更多功能 ...

 https://github.com/HACKERALERT/Picocrypt

[image]
[image]

加密、生成校验和销毁文件

[image] 关键词	加密 查询整理 身份验证
[image] 创建时间	2025年3月18日
[image] **Description**	工具

Picocrypt 是一款简单实用的工具，可用于加密文件、生成校验和销毁文件等。

Picocrypt 使用安全的 XChaCha20流密码和 Argon2加密算法来提供高级保护。

▫️Picocrypt 很小巧，仅 3MB

▫️Picocrypt 便携式（无需安装），不需要管理员/root 权限。

▫️Picocrypt 提供一个安全密码生成器，你可以用它来创建加密安全密码。

▫️Picocrypt 支持使用密钥文件作为额外（或唯一）的身份验证形式。

以及更多功能 ...

 https://github.com/HACKERALERT/Picocrypt

[image]
[image]

安卓下载器：下载音视频文件

[image] 关键词	安卓
[image] 创建时间	2025年3月19日
[image] **Description**	工具

YTDLnis 是一款 Android 应用程序，可从 1000 多个网站下载音频和视频文件，并提供播放列表处理和文件编辑等多种功能。

用户可以设置通用的下载格式、路径、名称模板，还有批量更新、下载时间表和多任务功能。

此外，还支持通过cookies授权下载私人视频，并支持时间戳剪切和元数据修改等编辑功能。

应用程序界面功能强大且可定制，支持 MVVM 架构、主题化以及数据备份和恢复功能。

https://github.com/deniscerri/ytdlnis

[image]
[image]

安卓下载器：下载音视频文件

[image] 关键词	安卓
[image] 创建时间	2025/03/19
[image] **Description**	工具

YTDLnis 是一款 Android 应用程序，可从 1000 多个网站下载音频和视频文件，并提供播放列表处理和文件编辑等多种功能。

用户可以设置通用的下载格式、路径、名称模板，还有批量更新、下载时间表和多任务功能。

此外，还支持通过cookies授权下载私人视频，并支持时间戳剪切和元数据修改等编辑功能。

应用程序界面功能强大且可定制，支持 MVVM 架构、主题化以及数据备份和恢复功能。

 https://github.com/deniscerri/ytdlnis

[image]
[image]

适用于多媒体的跨平台搜索引擎和文件资源管理器

[image] 关键词	元数据 查询整理 跨平台
[image] 创建时间	2025/03/22
[image] **Description**	工具

KFE 是一个跨平台的本地多媒体文件搜索引擎，由于数据不会离开用户的设备，因此隐私程度较高。

该程序支持通过CLIP 搜索多媒体文件，为音频和视频文件自动生成的转录，以及从图像中提取文本。

用户界面友好，便于查看和编辑元数据，可在 Mac、Linux 和 Windows 上离线运行。

该应用以不同模式将数据存储在可搜索的 SQLite 数据库中，并允许使用不同模型进行转录和文本提取。

 https://github.com/Fl0k3n/kfe

#tools #AI

[image]
[image]

适用于多媒体的跨平台搜索引擎和文件资源管理器

[image] 关键词	元数据 查询整理 跨平台
[image] 创建时间	2025年3月22日
[image] **Description**	工具

KFE 是一个跨平台的本地多媒体文件搜索引擎，由于数据不会离开用户的设备，因此隐私程度较高。

该程序支持通过CLIP 搜索多媒体文件，为音频和视频文件自动生成的转录，以及从图像中提取文本。

用户界面友好，便于查看和编辑元数据，可在 Mac、Linux 和 Windows 上离线运行。

该应用以不同模式将数据存储在可搜索的 SQLite 数据库中，并允许使用不同模型进行转录和文本提取。

 https://github.com/Fl0k3n/kfe

[image]
[image]

URL 检查

[image] 关键词	URL 免追踪 预防性
[image] 创建时间	2025/03/25
[image] **Description**	工具

URLCheck 是一款用于 URL 检查和自动化的免费 Android 应用程序。

URLCheck 是一款功能强大的自定义URL中介，可移除跟踪器、附属链接、不必要的元素、检查主机、防止某些网络钓鱼方法等。

开源免费无广告，只需互联网权限。

 https://github.com/TrianguloY/URLCheck

F-droid: https://f-droid.org/packages/com.trianguloy.urlchecker/

[image]
[image]

URL 检查

[image]	关键词	URL 免追踪 预防性
[image]	创建时间	2025年3月25日
[image]	**Description**	工具

URLCheck 是一款用于 URL 检查和自动化的免费 Android 应用程序。

URLCheck 是一款功能强大的自定义URL中介，可移除跟踪器、附属链接、不必要的元素、检查主机、防止某些网络钓鱼方法等。

开源免费无广告，只需互联网权限。

 https://github.com/TrianguloY/URLCheck

F-droid: https://f-droid.org/packages/com.trianguloy.urlchecker/

[image]
[image]

去中心化无服务器的匿名聊天

[image] 关键词	IMs 加密 去中心化 浏览器 自托管
[image] 关联	[image]一系列安全的即时通信软件和服务
[image] 创建时间	2025年3月26日
[image] **Description**	工具

Web Chat 是一个去中心化、无服务器的匿名聊天浏览器扩展程序，可使用 WebRTC 进行端到端加密通信，与任何网站上的用户聊天，并且所有数据都存储在本地，以提高隐私性。

安装后，用户会看到一个幽灵图标，单击它就可以在同一网站上与其他人聊天了

 https://github.com/molvqingtai/WebChat

[image]
[image]

去中心化无服务器的匿名聊天

[image] 关键词	IMs 加密 去中心化 浏览器 自托管
[image] 创建时间	2025/03/26
[image] **Description**	工具

Web Chat 是一个去中心化、无服务器的匿名聊天浏览器扩展程序，可使用 WebRTC 进行端到端加密通信，与任何网站上的用户聊天，并且所有数据都存储在本地，以提高隐私性。

安装后，用户会看到一个幽灵图标，单击它就可以在同一网站上与其他人聊天了

 https://github.com/molvqingtai/WebChat

[image]
[image]

命令行隐写工具

[image]	关键词	加密 隐写术
[image]	关联	[image]一系列隐写工具
[image]	创建时间	2025年4月8日
[image]	**Description**	工具

Stega Shade CLI 是一款易于使用的命令行隐写术工具，可以将信息隐藏在图像中。

支持使用 AES加密信息，从而确保传输数据的安全性。

该工具还包括高效的错误处理功能，可改善用户体验。

 https://github.com/merwin-asm/StegaShade

[image]
[image]

命令行隐写工具

[image] 关键词	加密 隐写术
[image] 创建时间	2025/04/08
[image] **Description**	工具

Stega Shade CLI 是一款易于使用的命令行隐写术工具，可以将信息隐藏在图像中。

支持使用 AES加密信息，从而确保传输数据的安全性。

该工具还包括高效的错误处理功能，可改善用户体验。

 https://github.com/merwin-asm/StegaShade

[image]
[image]

交互式高质量网页存档

[image] 关键词	查询整理 浏览器
[image] 关联	[image]一个功能强大的自托管 Internet 存档解决方案 ；[image]随手存档 ；
[image] 创建时间	2025年4月11日
[image] **Description**	工具

ArchiveWeb.page 是一款基于JavaScript的应用程序，可直接在浏览器中运行交互式高质量网页存档。
可作为谷歌浏览器的扩展程序使用，或者独立的Electron应用。

该扩展可在 Chrome 网上商店安装，桌面版可在 GitHub 上下载。

 https://github.com/webrecorder/archiveweb.page

[image]
[image]

交互式高质量网页存档

[image] 关键词	查询整理 浏览器
[image] 创建时间	2025/04/11
[image] Description	工具

ArchiveWeb.page 是一款基于JavaScript的应用程序，可直接在浏览器中运行交互式高质量网页存档。
可作为谷歌浏览器的扩展程序使用，或者独立的Electron应用。

该扩展可在 Chrome 网上商店安装，桌面版可在 GitHub 上下载。

 https://github.com/webrecorder/archiveweb.page

[image]
[image]

创建和注入浏览器指纹

[image] 关键词	免追踪 对抗性思考方式 浏览器
[image] 创建时间	2025/04/14
[image] **Description**	工具

Fingerprint-suite 是一套用于创建和注入浏览器指纹的工具，可帮助用户绕过网站上的跟踪。

 https://github.com/apify/fingerprint-suite

#tools

[image]
[image]

创建和注入浏览器指纹

[image] 关键词	免追踪 对抗性思考方式 浏览器
[image] 创建时间	2025年4月14日
[image] **Description**	工具

Fingerprint-suite 是一套用于创建和注入浏览器指纹的工具，可帮助用户绕过网站上的跟踪。

 https://github.com/apify/fingerprint-suite

#tools

[image]
[image]

免费下载工具

[image] 关键词	效率
[image] 创建时间	2025年4月15日
[image] **Description**	工具

Cobalt 是一款用户友好型媒体下载工具，没有广告没有付费墙，用户只需粘贴链接即可下载文件。

 https://github.com/imputnet/cobalt

网站： https://cobalt.tools/

[image]
[image]

免费下载工具

[image] 关键词		效率
[image] 创建时间		2025/04/15
[image] **Description**		工具

Cobalt 是一款用户友好型媒体下载工具，没有广告没有付费墙，用户只需粘贴链接即可下载文件。

 https://github.com/imputnet/cobalt

网站： https://cobalt.tools/

[image]
[image]

在本地运行AI

[image] 关键词	AI 自托管
[image] 创建时间	2025/04/17
[image] **Description**	工具

1. llama.cpp (https://github.com/ggerganov/llama.cpp) - 纯 C/C++ 的 LLaMA，可在本地 CPU 上运行；

1. Jan (https://github.com/janhq/jan) - ChatGPT 的开源替代方案，可在电脑上 100% 离线运行；

1. LocalAI (https://github.com/mudler/LocalAI) - OpenAI、Claude 等人的免费开源替代品。自托管且本地优先，用 Go 编写；

1. ollama (https://github.com/ollama/ollama) - 用于在本地级别使用 Llama 2 和其他主要语言模型的工具；

1. LM Studio (https://lmstudio.ai/) - 用于探索、加载和运行各种大型语言模型（LLM）的软件；

1. llamafile (https://github.com/Mozilla-Ocho/llamafile) - 允许您在单个文件中运行不同的 LLM；

1. GPT4ALL (https://www.nomic.ai/gpt4all) - 另一个本地运行 ChatGPT 的著名解决方案。

[image]
[image]

在本地运行AI

[image]	关键词	AI 自托管
[image]	创建时间	2025年4月17日
[image]	**Description**	工具

1. llama.cpp (https://github.com/ggerganov/llama.cpp) - 纯 C/C++ 的 LLaMA，可在本地 CPU 上运行；

1. Jan (https://github.com/janhq/jan) - ChatGPT 的开源替代方案，可在电脑上 100% 离线运行；

1. LocalAI (https://github.com/mudler/LocalAI) - OpenAI、Claude 等人的免费开源替代品。自托管且本地优先，用 Go 编写；

1. ollama (https://github.com/ollama/ollama) - 用于在本地级别使用 Llama 2 和其他主要语言模型的工具；

1. LM Studio (https://lmstudio.ai/) - 用于探索、加载和运行各种大型语言模型（LLM）的软件；

1. llamafile (https://github.com/Mozilla-Ocho/llamafile) - 允许您在单个文件中运行不同的 LLM；

1. GPT4ALL (https://www.nomic.ai/gpt4all) - 另一个本地运行 ChatGPT 的著名解决方案。

[image]
[image]

在视频中嵌入隐藏水印

[image] 关键词	AI 效率
[image] 创建时间	2025/04/22
[image] **Description**	工具

Video Seal 是一款在视频中嵌入隐藏水印的人工智能工具。

Video Seal 可应用于从隐写术到版权保护等多种领域 ......

 https://github.com/facebookresearch/videoseal

演示：https://aidemos.meta.com/videoseal

[image]
[image]

在视频中嵌入隐藏水印

[image] 关键词	AI 效率
[image] 创建时间	2025年4月22日
[image] **Description**	工具

Video Seal 是一款在视频中嵌入隐藏水印的人工智能工具。

Video Seal 可应用于从隐写术到版权保护等多种领域 ……

 https://github.com/facebookresearch/videoseal

演示：https://aidemos.meta.com/videoseal

[image]
[image]

匿名 SIM/SMS 服务

[image] 关键词	SMS 免追踪 加密
[image] 创建时间	2025/05/09
[image] **Description**	工具

1. Simsup (https://simsup.net/)- 在全球销售匿名 SIM 卡的服务。付款方式为 XMR/BTC。

1. sms4sats (https://sms4sats.com/) - 国外流行的短信接收服务。

1. Crypton (https://crypton.sh/) - 提供匿名 SIM 卡的服务, 256 加密。

1. JMP (https://jmp.chat/) - 通过 XMPP 发送短信和拨打电话的服务。

1. Monerosms (https://monerosms.com/) - 发送匿名短信，以 XMR 支付。

1. smspool (https://www.smspool.net/) | juicysms (https://juicysms.com/) | textverified (https://www.textverified.com/) - 更多短信接收服务。

[image]
[image]

匿名 SIM/SMS 服务

[image]	关键词	SMS 免追踪 加密
[image]	关联	离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线P2P安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；网状网络通信，支持LoRa 设备
[image]	创建时间	2025年5月9日
[image]	**Description**	工具

1. Simsup (https://simsup.net/)- 在全球销售匿名 SIM 卡的服务。付款方式为 XMR/BTC。

1. sms4sats (https://sms4sats.com/) - 国外流行的短信接收服务。

1. Crypton (https://crypton.sh/) - 提供匿名 SIM 卡的服务, 256 加密。

1. JMP (https://jmp.chat/) - 通过 XMPP 发送短信和拨打电话的服务。

1. Monerosms (https://monerosms.com/) - 发送匿名短信，以 XMR 支付。

1. smspool (https://www.smspool.net/) | juicysms (https://

juicysms.com/) | textverified (https://www.textverified.com/) - 更多短信接收服务。

[image]
[image]

将电子书转换为有声读物

[image]	关键词	倡导活动 效率
[image]	创建时间	2025/05/15
[image]	**Description**	工具

ebook2audiobook 是一款使用 Calibre 和 ffmpeg 等程序将电子书转换为有声读物的工具，支持章节和元数据。

该工具允许语音克隆，支持一千多种语言，但只适用于无版权保护的书籍。

它的主要功能包括转换为文本格式、将音频整理成章节和高质量语音合成。该工具至少需要 4GB 内存，web界面和 Docker 支持。

 https://github.com/DrewThomasson/ebook2audiobook

[image]
[image]

将电子书转换为有声读物

[image] 关键词		倡导活动 效率
[image] 创建时间		2025年5月15日
[image] **Description**		工具

ebook2audiobook 是一款使用 Calibre 和 ffmpeg 等程序将电子书转换为有声读物的工具，支持章节和元数据。

该工具允许语音克隆，支持一千多种语言，但只适用于无版权保护的书籍。

它的主要功能包括转换为文本格式、将音频整理成章节和高质量语音合成。该工具至少需要 4GB 内存，web界面和 Docker 支持。

 https://github.com/DrewThomasson/ebook2audiobook

[image]
[image]

隐私设置终极指南

[image] 关键词	自助 预防性
[image] 创建时间	2025/05/16
[image] **Description**	工具

StellarSand/privacy-settings 是热门应用程序、账户和服务中隐私设置的终极指南。

您可以在这里找到浏览器、电子邮件客户端、Telegram、YouTube、X、Instagram 等等的实际设置建议。

但请记住，隐私设置并不是万能的，它只是一个基础。

https://github.com/StellarSand/privacy-settings

[image]
[image]

隐私设置终极指南

[image] 关键词	自助 预防性
[image] 创建时间	2025年5月16日
[image] **Description**	工具

StellarSand/privacy-settings 是热门应用程序、账户和服务中隐私设置的终极指南。

您可以在这里找到浏览器、电子邮件客户端、Telegram、YouTube、X、Instagram 等等的实际设置建议。

但请记住，隐私设置并不是万能的，它只是一个基础。

 https://github.com/StellarSand/privacy-settings

[image]
[image]

清除 Windows 11 中所有垃圾

[image] 关键词	反侦察 电脑
[image] 创建时间	2025年5月22日
[image] **Description**	工具

Win11Debloat 是一款能清除 Windows 11 中所有垃圾的实用工具。

- 删除所有无用的应用程序和实用程序；
- 禁用广告和遥测等功能；
- 删除起始菜单中所有固定的应用程序；
- 显示隐藏的文件和文件夹；
- 恢复旧的 Windows10 样式上下文菜单；
  及其他。

在 PowerShell 终端中运行。

 https://github.com/Raphire/Win11Debloat

[image]
[image]

清除 Windows 11 中所有垃圾

[image]	关键词	反侦察 电脑
[image]	创建时间	2025/05/22
[image]	**Description**	工具

Win11Debloat 是一款能清除 Windows 11 中所有垃圾的实用工具。

- 删除所有无用的应用程序和实用程序；
- 禁用广告和遥测等功能；
- 删除起始菜单中所有固定的应用程序；
- 显示隐藏的文件和文件夹；
- 恢复旧的 Windows10 样式上下文菜单；
  及其他。

在 PowerShell 终端中运行。

 https://github.com/Raphire/Win11Debloat

[image]
[image]

去中心化 P2P 聊天应用

[image] 关键词	IMs P2P 加密 去中心化
[image] 创建时间	2025/06/06
[image] **Description**	工具

Chitchatter 是一款用于创建去中心化 P2P 聊天的应用程序，在聊天过程中，参与者无需访问中心化服务器即可直接进行交互。

该应用程序允许您生成一个唯一的聊天标识符，将其传递给其他参与者即可开始通信。任何支持 WebTorrent 协议的公共服务器都可用于连接。

通信内容不会保存，一旦用户关闭页面或离开聊天室，对话记录就会从本地内存中删除。

可自托管。可嵌入。

 https://chitchatter.im/

[image]
[image]

去中心化 P2P 聊天应用

[image] 关键词	IMs P2P 加密 去中心化
[image] 关联	[image]一系列安全的即时通信软件和服务 ；离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线P2P安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；网状网络通信，支持LoRa 设备
[image] 创建时间	2025年6月6日
[image] **Description**	工具

Chitchatter 是一款用于创建去中心化 P2P 聊天的应用程序，在聊天过程中，参与者无需访问中心化服务器即可直接进行交互。

该应用程序允许您生成一个唯一的聊天标识符，将其传递给其他参与者即可开始通信。任何支持 WebTorrent 协议的公共服务器都可用于连接。

通信内容不会保存，一旦用户关闭页面或离开聊天室，对话记录就会从本地内存中删除。

可自托管。可嵌入。

 https://chitchatter.im/

[image]
[image]

看视频学外语

[image] 关键词	AI 学习
[image] 创建时间	2025/06/10
[image] **Description**	工具

LLPlayer 是一款专为语言学习者设计的独特视频播放器。

它具有许多重要功能，例如可同时显示文本字幕和位图字幕、使用 OpenAI Whisper 自动生成 100 种语言的字幕，以及与谷歌 API 和 DeepL 集成以翻译成 134 种语言。

此外，OCR 功能可将位图字幕实时转换为文本字幕。

该播放器可在 Windows 10 和 11 上运行。

 https://github.com/umlx5h/LLPlayer

[image]
[image]

看视频学外语

[image] 关键词	AI 学习
[image] 创建时间	2025年6月10日
[image] **Description**	工具

LLPlayer 是一款专为语言学习者设计的独特视频播放器。

它具有许多重要功能，例如可同时显示文本字幕和位图字幕、使用 OpenAI Whisper 自动生成 100 种语言的字幕，以及与谷歌 API 和 DeepL 集成以翻译成 134 种语言。

此外，OCR 功能可将位图字幕实时转换为文本字幕。

该播放器可在 Windows 10 和 11 上运行。

 https://github.com/umlx5h/LLPlayer

[image]
[image]

极简发布平台

[image] 关键词		倡导活动
[image] 创建时间		2025年6月18日
[image] **Description**		工具

TapNote 是一个极简的发布平台，灵感来自 Telegra.ph，可使用 Markdown 创建内容。

它提供简洁的写作体验，无需创建账户即可即时发布笔记、博客和其他文档。

TapNote 的主要功能包括 Markdown 的易用性、自托管和完整的内容管理、每篇文章的唯一 URL 以及对图片和代码片段的支持。

TapNote 使用 Django、Tailwind CSS 和 Google Fonts 开发。

 https://github.com/vorniches/tapnote

[image]
[image]

极简发布平台

[image] 关键词	倡导活动
[image] 创建时间	2025/06/18
[image] **Description**	工具

TapNote 是一个极简的发布平台，灵感来自 Telegra.ph ，可使用 Markdown 创建内容。

它提供简洁的写作体验，无需创建账户即可即时发布笔记、博客和其他文档。

TapNote 的主要功能包括 Markdown 的易用性、自托管和完整的内容管理、每篇文章的唯一 URL 以及对图片和代码片段的支持。

TapNote 使用 Django、Tailwind CSS 和 Google Fonts 开发。

 https://github.com/vorniches/tapnote

[image]
[image]

安全的秘密共享

[image] 关键词	传输安全 加密
[image] 关联	[image]在不安全渠道上尽可能安全地共享秘密 ；[image]在不同操作系统之间传输文件 ；[image]一些私密安全的文件传输解决方案 ；[image]在任何聊天工具中发送算对端加密信息 ；[image]安全共享 ；
[image] 创建时间	2025年6月23日
[image] **Description**	工具

DiceSlice 是一个web应用，通过加密和将数据分割成“切片文件”，实现安全的秘密共享。

它使用 AES-256/GCM 和Shamir秘密共享算法来确保信息安全，所有操作均离线执行。

目前还在开发中，计划引更多新功能，如非对称切片文件支持和密码保护等。

主要限制包括加密数据的最大大小（约 2 GB）。

 https://github.com/numago/diceslice

[image]
[image]

安全的秘密共享

[image] 关键词	传输安全 加密
[image] 创建时间	2025/06/23
[image] **Description**	工具

DiceSlice 是一个web应用，通过加密和将数据分割成“切片文件”，实现安全的秘密共享。

它使用 AES-256/GCM 和Shamir秘密共享算法来确保信息安全，所有操作均离线执行。

目前还在开发中，计划引更多新功能，如非对称切片文件支持和密码保护等。

主要限制包括加密数据的最大大小（约 2 GB）。

 https://github.com/numago/diceslice

[image]
[image]

Telegram 语音笔记转录和摘要机器人

[image] 关键词	telegram 效率
[image] 创建时间	2025/07/02
[image] **Description**	工具

这是一款 Telegram 机器人，使用人工智能模型来转录和总结语音笔记。

该机器人使用 Python 构建，集成了 Groq API 以及 Whisper 和 Llama 3 模型。

它能够转录语音信息并创建简短摘要，支持多种音频格式，并提供易于使用的输出。

 https://github.com/aviaryan/voice-transcribe-summarize-telegram-bot

[image]
[image]

Telegram 语音笔记转录和摘要机器人

[image]	关键词	telegram 效率
[image]	关联	[image]Telegram内容提取工具；[image]Telegram 语音笔记转录和摘要机器人；[image]把你的Telegram变成无限云存储
[image]	创建时间	2025年7月2日
[image]	**Description**	工具

这是一款 Telegram 机器人，使用人工智能模型来转录和总结语音笔记。

该机器人使用 Python 构建，集成了 Groq API 以及 Whisper 和 Llama 3 模型。

它能够转录语音信息并创建简短摘要，支持多种音频格式，并提供易于使用的输出。

 https://github.com/aviaryan/voice-transcribe-summarize-telegram-bot

[image]
[image]

云存储文件管理

[image] 关键词	云存储 查询整理
[image] 创建时间	2025年7月3日
[image] **Description**	工具

Cloud Storage Manager 是一款基于网络的现代云存储文件管理应用程序，提供直观的界面和一系列功能，如拖放文件上传、通过临时 URL 安全共享以及针对移动设备的自适应设计。

它支持多种云提供商，包括亚马逊 S3、谷歌云存储等，用户可以根据成本和性能标准选择最佳方案。

该应用程序使用 Flask 和 AWS S3，JavaScript 和 Bootstrap，通过凭证管理提供安全性。

 https://github.com/rohitg00/s3-file-share-for-free

[image]
[image]

云存储文件管理

[image]	关键词	云存储 查询整理
[image]	创建时间	2025/07/03
[image]	**Description**	工具

Cloud Storage Manager 是一款基于网络的现代云存储文件管理应用程序，提供直观的界面和一系列功能，如拖放文件上传、通过临时 URL 安全共享以及针对移动设备的自适应设计。

它支持多种云提供商，包括亚马逊 S3、谷歌云存储等，用户可以根据成本和性能标准选择最佳方案。

该应用程序使用 Flask 和 AWS S3，JavaScript 和 Bootstrap，通过凭证管理提供安全性。

 https://github.com/rohitg00/s3-file-share-for-free

[image]
[image]

安全文件存储

[image]	关键词	加密 查询整理
[image]	创建时间	2025年7月4日
[image]	**Description**	工具

MyDrive 是一款开源云文件存储服务器（类似于 Google Drive），可让您使用网络浏览器操作在您自己的服务器或安全平台上托管的数据。

主要功能包括文件上传和下载、支持各种数据库、媒体浏览，AES256 加密。使用 React、Typescript 和 Node.js 技术进行开发。

□ https://github.com/subnub/myDrive

[image]
[image]

安全文件存储

[image]	关键词	加密 查询整理
[image]	创建时间	2025/07/04
[image]	**Description**	工具

MyDrive 是一款开源云文件存储服务器（类似于 Google Drive），可让您使用网络浏览器操作在您自己的服务器或安全平台上托管的数据。

主要功能包括文件上传和下载、支持各种数据库、媒体浏览，AES256 加密。使用 React、Typescript 和 Node.js 技术进行开发。

 https://github.com/subnub/myDrive

[image]
[image]

带有频道功能的离线P2P安全通信

[image] 关键词	IMs P2P 加密 团队 离线
[image] 创建时间	2025年7月11日
[image] **Description**	工具

bitchat — 由前Twitter联合创始人杰克多尔西开发的网状网络P2P即时通讯应用。无需互联网连接即可使用。

功能：

1. 去中心化网状网络：通过蓝牙 LE 自动发现用户并传输消息；

1. 端到端加密：使用 X25519 + AES-256-GCM 密钥交换进行个人消息传输；

1. 基于频道的聊天：按主题进行群组消息交换，并提供额外的密码保护；

1. 消息存储与转发：消息会被缓存以供离线用户使用，并在他们重新连接时送达；

1. 完全隐私：无需电话号码、ID 或账户；

1. IRC 风格命令：熟悉的 /join、/msg、/who 等命令界面；

1. 消息保存：可选的整个频道消息保存功能，由频道所有者控制；

1. 流量掩护：定时混淆和虚拟消息以提高隐私性；

1. 紧急清除：三次点击即可立即清除所有数据。

 https://github.com/permissionlesstech/bitchat?tab=readme-ov-file

该项目目前仍处于开发阶段，但听起来很有前景。

建议评估已实现的类似项目。 BACK 返回：[image]一系列安全的即时通信软件和服务

[image]
[image]

一些安全存储照片的方法 [Android版]

[image]	关键词	存储安全 安卓 自主 自托管
[image]	创建时间	2025年7月11日
[image]	**Description**	工具

自主解决方案

Immich (WIP) ：https://github.com/immich-app/immich

LibrePhotos：https://github.com/LibrePhotos/librephotos

Nextcloud：https://nextcloud.com/

PhotoPrism：https://www.photoprism.app/

Pigallery2：https://bpatrik.github.io/pigallery2/

Photoview：https://photoview.github.io/

Photostructure：https://photostructure.com/

本地解决方案

digiKam：https://www.digikam.org/

Photok：https://github.com/leonlatsch/Photok

ImageGlass：https://imageglass.org

[image]
[image]

绕开KYC 的情况下用加密货币交换加密货币的方法

[image] 关键词	加密货币 身份验证
[image] 关联	[image]免 KYC 的交易平台（精选）；[image]调查区块链上的交易；**绕开KYC** 的情况下用加密货币交换加密货币的方法；隐私堡垒门罗币 - 服务清单**2026**：钱包、交易所、匿名**SIM**卡、主机及其他
[image] 创建时间	2025年7月13日
[image] **Description**	工具

KYC是一个许多金融机构所要求的身份验证过程，包括加密货币交易所。其目的是确认客户的身份。

以下是一些绕开KYC的可能性。不要做任何伤害性事件！

1. https://www.wizardswap.pw

2. https://bitcoinvn.io/

3. https://basicswapdex.com/

4. https://crp.is/

5. https://stealthex.io/

1. https://unstoppableswap.net/

1. https://robosats.org

1. https://bisq.network

1. https://exch.net/

1. https://swapter.io/

[image]
[image]

像1984那样通信

[image]	关键词	反封锁
[image]	创建时间	2025年7月16日
[image]	**Description**	工具

neo146 是一个实验性的消息网关，旨在提供应急通信。

它提供两种类型的网关：HTTP-SMS 和 HTTP-Markdown，允许用户通过 SMS 接收来自各种互联网来源的信息。

所有短信响应都经过 base64 编码优化，长消息会被分成多个部分。

 https://github.com/ooguz/neo146

[image]
[image]

离线求救

[image] 关键词	个人 气候灾难 自助
[image] 创建时间	2025年7月18日
[image] **Description**	工具

Igatha 是一款开源离线的SOS应用，它专为军事冲突和灾难中发送求救信号和重新连接而设计。

它允许用户使用蓝牙低功耗技术发送求救信号，无需互联网或GPS即可传输信息，在紧急情况下也能发挥作用。

此外，设备的扬声器还会发出警报声，帮助救援人员找到你。

此外，Igatha 还能通过设备上的传感器（加速计、陀螺仪和气压计）探测灾难。

当多个传感器同时检测到突变时，就会触发灾难检测系统。

 https://github.com/nizarmah/igatha

[image]
[image]

Telegram内容提取工具

[image] 关键词	IMs OSINT telegram 查询整理
[image] 关联	[image]Telegram 语音笔记转录和摘要机器人 ；[image]Telegram探索工具 ；[image]把你的Telegram变成无限云存储
[image] 创建时间	2025年7月24日
[image] Description	工具

Telegraphite 是一款功能强大的工具，用于从公开 Telegram 源中提取和保存帖子，具有多种功能。

它支持从多个频道提取帖子、以 JSON 格式保存数据、上传媒体文件和按关键字过滤。

该工具可在计划模式和连续模式下运行，并能删除重复的帖子。

可按关键字或内容类型（纯文本、纯媒体）筛选。

数据存储在结构化目录中，每个 posts.json 文件都包含帖子信息，如ID、日期和内容。

 https://github.com/hamodywe/telegram-scraper-TeleGraphite

[image]
[image]

自检URL阻止恶意网站

[image] 关键词	病毒检测 监测 自检
[image] 创建时间	2025年7月27日
[image] **Description**	工具

Osprey 是一个浏览器扩展，可使用 Microsoft SmartScreen 和 Norton SafeWeb 等工具提供保护，防止恶意网站的入侵。

它能自动检查 URL 并阻止被识别为有害的网站，包括网络钓鱼和诈骗网站。

如果检测到威胁，会向用户发出警告。

 https://github.com/Foulest/Osprey

[image]
[image]

在 Docker 中运行 macOS虚拟机

[image] 关键词	电脑 虚拟机
[image] 创建时间	2025年8月5日
[image] **Description**	工具

Lumier 是一个允许您在 Docker 中运行 macOS虚拟机的项目，为使用 macOS 应用程序提供了一种方便灵活的方式。

▫ 几分钟内即可获得即用型 macOS 虚拟机。

▫ 通过VNC基于浏览器访问虚拟机。

▫ 在主机和虚拟机之间共享文件。

▫ 通过环境变量轻松配置。

 https://github.com/trycua/cua/tree/main/libs/lumier

[image]
[image]

专为保护您的照片而设计的相机应用

[image] 关键词	传输安全 加密 反审查 存储安全 移动设备 预防性
[image] 创建时间	2025年8月6日
[image] **Description**	工具

Snap Safe 是智能手机安全相机的一个很好的变体；

- 照片不会显示在图库中，而是加密存储；
- 可设置一个特殊的 PIN（Poison Pill），输入后会删除所有照片；
- 同时可预设无害的 "诱饵照片"，这些照片可以在您被迫采取 Poison Pill 时不会被强制删除，以帮助您掩盖删除动作；
- 使用安全模糊算法自动模糊人脸；
- 分享时自动清除照片中的所有元数据；

以及更多功能。

 https://github.com/SecureCamera/SecureCameraAndroid

[image]
[image]

安卓 - 简单易用的隐私管理器

[image]	关键词	安卓 移动设备 自助 预防性
[image]	创建时间	2025年8月7日
[image]	**Description**	工具

XPL-EX（XPrivacy Lua EX）是一款开源安卓（6.0+）应用程序，基于 M66B 的 XPrivacyLua，用于隐私保护。

它使用 Xposed 框架来挂钩（拦截）API 调用，防止应用程序访问敏感的设备数据（如 IMEI、位置、联系人）。

用户可以使用 Lua 脚本配置钩子，指定应用程序的行为。XPL-EX 完全免费，无广告、无分析、无服务器连接。

 https://github.com/0bbedCode/XPL-EX

[image]
[image]

加密的安卓位置共享

[image] 关键词	tor 加密 安卓 定位 移动设备
[image] 关联	🔎 与可信赖的朋友安全地共享位置
[image] 创建时间	2025年8月8日
[image] **Description**	工具

Find Family 是一款为家人和朋友提供端到端加密的安卓位置共享应用程序。

它无需用户提供个人信息，就能提供高度的隐私保护。

该应用的主要功能包括临时启用或禁用位置共享、在前往已保存的位置时接收通知、跟踪电池状态和共享当前速度。

用户可以查看在特定地点停留的时间，并查看位置历史记录。

此外，还支持通过链接临时共享、蓝牙设备跟踪和通过Tor连接，从而使该应用程序更加安全和私密。

 https://github.com/vayun-mathur/Find-Family

[image]
[image]

安卓隐私浏览器

[image] 关键词		安卓 数据最小化 浏览器 移动设备
[image] 创建时间		2025年8月11日
[image] **Description**		工具

Privacy Browser 是一款不错的注重隐私的浏览器。适用于安卓用户。

可最大限度地减少发送到互联网和本地存储的数据。

功能：

- EasyList 集成广告拦截器；
- 支持 Tor Orbot 代理服务器；
- 附加 SSL 证书；
- 导入/导出设置和书签；

 https://f-droid.org/en/packages/com.stoutner.privacybrowser.standard/

[image]
[image]

终端上的 AI Agent

[image] 关键词	AI 个人
[image] 创建时间	2025年8月12日
[image] **Description**	工具

Dasshh 是一款开源的TUI 应用程序，可让您使用自然语言与计算机进行交互。

其主要功能包括用简单的英语执行系统命令 、以对话方式管理文件和目录、自动执行重复性任务、语法高亮显示 …… 以及集成可扩展工具和在无图形用户界面的终端中工作的能力。

 https://github.com/vgnshiyer/dasshh

[image]
[image]

强制加密密钥 USB 存储

[image] 关键词	存储安全 身份验证
[image] 创建时间	2025年8月13日
[image] **Description**	工具

PECKUS 是一款由用户激活的 USB 设备，用于使用 CircuitPython 存储密码密钥等文件。

只有在确认授权用户在场后才能访问存储设备，这大大提高了数据的安全性。

设备在闲置一段时间后会自动锁定，从而提供了额外的保护。

 https://github.com/juergenpabel/circuitpython-peckus

[image]
[image]

实时语音翻译

[image] 关键词	AI 无障碍 翻译 自主
[image] 关联	[image]翻译视频 ；[image]一些可选的翻译服务 ；[image]一系列免费的人工智能翻译器 ；[image]跨平台AI翻译
[image] 创建时间	2025年8月19日
[image] Description	工具

Sokuji 是一款使用 OpenAI 实时 API 进行实时语音翻译的桌面应用程序。

它通过实时捕捉和处理音频输入，帮助打弥合真实对话中的语言障碍。

除桌面应用程序外，Sokuji 还为 Chrome 浏览器和基于 Chromium 的浏览器提供扩展功能，可与 Google Meet 和 Microsoft Teams 集成。

https://github.com/kizuna-ai-lab/sokuji

[image]
[image]

寻找代码中的漏洞

[image]	关键词	开发者 自检 预防性
[image]	创建时间	2025年8月20日
[image]	**Description**	工具

Bandit 是一款 Python 代码安全分析工具，旨在检测常见漏洞。

它能构建抽象语法树，应用插件进行详细扫描，并根据扫描结果生成报告。

Bandit 以容器镜像的形式提供，支持多种架构。

https://github.com/PyCQA/bandit

[image]
[image]

Google Drive 的开源替代产品

[image]	关键词	存储安全 开源 文件处理
[image]	创建时间	2025年8月21日
[image]	**Description**	工具

Nimbus 云存储是 Google Drive 的开源替代产品，为用户提供远程安全存储和管理数据的能力。

该项目支持与 PostgreSQL 集成，并提供灵活的定制选项。Nimbus 面向希望使用开源解决方案满足其需求的开发人员。

 https://github.com/logscore/Nimbus

[image]
[image]

适用于移动设备的Tor浏览器精选

[image] 关键词	tor 个人 移动设备
[image] 关联	[image]从普通浏览器进入Tor网络;
[image] 创建时间	2025年8月22日
[image] Description	工具

安卓

1. Tor Browser - 官方客户端，运行正常，也可从 F-Droid 安装；

2. orbot - 通过它重定向其他应用程序的流量到Tor；

3. orNET Browser - 非官方客户端，内置 VPN 和 JS 切换功能；

iOS

1. orNET 浏览器 - 开源浏览器，可让您通过 iOS 设备访问 Tor 网络。已获得 Tor 项目批准；

2. Purple Onion - 另一款由 Tor 支持的付费无广告浏览器；

3. Incognito TOR 浏览器 - 非官方的浏览器，具有额外功能，付费，但有试用版。

[image]
[image]

把手机变成临时USB记忆棒

[image] 关键词	存储安全 安卓 转储
[image] 创建时间	2025年8月25日
[image] **Description**	工具

Transfer 是一款简单易用的安卓应用程序，可通过Wi-Fi快速上传和下载文件，将您的智能手机变成一个可在任何设备上通过浏览器访问的临时USB驱动器。

它简化了本地网络上的文件共享，无需使用 USB 驱动器和云服务。

主要功能包括通过 HTTP 轻松共享文件、IP 限制和密码安全设置。

应用程序界面直观，设置过程简单，无需连接互联网。

 https://github.com/matan-h/Transfer

[image]
[image]

高安全度终端私密聊天

[image] 关键词	IMs 加密 电脑 自托管
[image] 关联	[image]一系列安全的即时通信软件和服务 ；离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线**P2P**安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；网状网络通信，支持**LoRa** 设备
[image] 创建时间	2025年8月26日
[image] **Description**	工具

Enchat 是一款私密的加密通信工具。

它的主要功能包括无账户、强大的 AES-256 加密、以及为每个会话创建唯一的临时密钥。

会话结束后，信息将无法访问，用户名和时间戳也会被加密。

该工具提供最大 5MB 的安全文件共享，通过 Tor 实现匿名，跨平台支持。

加密在用户的设备上进行，以确保内容安全。

Enchat兼容Python 3.6及以上版本，可在Linux、macOS和Windows上运行。可使用强口令及设置自己的服务器以获得更高的安全性。

 https://github.com/sudodevdante/enchat

[image]
[image]

私密P2P的团队IM，无需服务器

[image] 关键词	IMs tor 加密 移动设备
[image] 关联	[image]一系列安全的即时通信软件和服务 ；离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线**P2P**安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；网状网络通信，支持**LoRa** 设备
[image] 创建时间	2025年8月27日
[image] **Description**	工具

Quiet 是 Slack、Discord 等团队聊天应用程序的加密 P2P 替代软件，基于 Tor 和 IPFS，无需服务器即可运行。

它专为重视去中心化和隐私的用户设计，允许设备之间直接交换信息。

每个社区都有自己独立的网络，确保数据得到保护。

主要功能包括端到端加密、社区访问控制、聊天组织、频道、文件发送支持以及 Android 和 iOS 移动应用程序。

 https://github.com/TryQuiet/quiet

[image]
[image]

开源防病毒软件精选

[image]	关键词	病毒检测 自助
[image]	创建时间	2025年8月28日
[image]	**Description**	工具

1. ClamAV (https://www.clamav.net/)

2. Bitdefender (https://www.bitdefender.com/en-us/consumer/free-antivirus)

3. MoonSecure （https://moonsecure.org/df/)

4. The OpenAntivirus Project （https://sourceforge.net/projects/openantivirus/)

5. The Rootkit Hunter (https://rkhunter.sourceforge.net/)

在线工具：

Hybrid Analysis (https://www.hybrid-analysis.com/)

Virus Total (https://www.virustotal.com/gui/home/upload)

MetaDefender Cloud (https://metadefender.opswat.com/)

[image]
[image]

安全的虚拟浏览器

[image]	关键词	团队 浏览器 电脑
[image]	创建时间	2025年9月1日
[image]	**Description**	工具

Neko 是在 Docker 中运行的虚拟浏览器，使用 WebRTC 安全、私密地访问互联网。

它不仅能让用户浏览网页，还能运行应用程序和执行其他任务，无论您是希望测试 Web 应用程序的开发人员， 还是寻求安全浏览体验的注重隐私的用户，或者只是想要利用虚拟浏览器的便利性和灵活性的人，都适合使用。

使用 Neko，您可以组织协作视频浏览、互动演示和支持多用户。

其优点包括流畅的视频、音频反馈，以及为匿名活动创建 "临时"浏览器。

 https://github.com/m1k1o/neko

[image]
[image]

AI文档处理工具

[image] 关键词	AI 文件处理
[image] 创建时间	2025年9月3日
[image] **Description**	工具

PDFY 是一个用 Rust 编写的简约命令行工具，它使用人工智能功能搜索 PDF 文档中的信息，并以 JSON 格式返回结果。

利用该工具，用户可以根据指定的查询从PDF中提取信息。

该工具为处理文档提供了友好的用户界面，并可集成到各种工作流程中。

 https://github.com/jdiaz97/pdfy

延伸：https://web.archive.org/web/20220125202402/https://www.iyouport.org/%E5%A6%82%E4%BD%95%E8%BF%8E%E6%8E%A5%E6%9B%B4%E5%A4%9A%E7%9A%84%E5%B7%B4%E6%8B%BF%E9%A9%AC%E6%96%87%E4%BB%B6%EF%BC%9F/

[image]
[image]

适合高风险用户的通信平台

[image] 关键词	IMs tor 加密 团队 自托管
[image] 关联	[image]一系列安全的即时通信软件和服务
[image] 创建时间	2025年9月4日
[image] **Description**	工具

Hush Line 是一个匿名通信平台，适用于记者、吹哨人、律师等在较高风险环境下工作的人。

功能：

- OCR Vision Assistant
- Tor Onion Service
- Proton Mail 密钥导入
- 端到端加密
- 自验证 URL
- 使用 Rise Up 作为邮件
- Mailvelope 集成

- 别名
- 基于 TOTR 的 2-FA

 https://hushline.app/

[image]
[image]

将数字本文转换为手写字体

[image] 关键词	笔迹鉴定
[image] 关联	✍笔迹分析
[image] 创建时间	2025年9月5日
[image] **Description**	工具

DeepScript 是一个可以将数字文本转换为独特手写字体的项目。

用户可以选择现成的字体或上传自己的手稿样本。

生成的文件可以预览和下载。

如果您想要制作手写海报、喷漆涂鸦、手写传单等，又担心被字体识别暴露身份，类似这样的工具可以派上用场。

https://github.com/dovbyk/DeepScript

[image]
[image]

谷歌“查找我的设备”的安全开源替代

[image] 关键词	开源 移动设备 谷歌 防盗
[image] 创建时间	2025年9月8日
[image] **Description**	工具

FMD Android 是谷歌“查找我的设备”（Find my Device）的安全开源替代软件，可为用户提供跟踪和管理设备的可靠解决方案。

FMD 的主要功能包括定位设备、锁定设备、打开声音、触发相机快照和出厂重置。

用户可以通过短信或 FMD Server 网页界面进行管理，还可以设置可信联系人和通过 PIN 匿名访问。

 https://gitlab.com/fmd-foss/fmd-android

 F-droid: https://f-droid.org/packages/de.nulide.findmydevice/

[image]
[image]

安全的剪贴板

[image] 关键词	剪贴板 加密 存储安全
[image] 创建时间	2025年9月9日
[image] **Description**	工具

Clip Vault 是一款使用 Rust 和 Tauri 开发的跨平台安全剪贴板，可使用 SQLCipher 自动加密剪贴板历史记录。

兼容 macOS、Windows 和 Linux，可通过全局热键快速搜索和访问项目。

所有数据均使用 AES-256 加密，没有明文存储的密码，数据库也是安全的。

 https://github.com/densumesh/clip-vault

[image]
[image]

自托管文件转换

[image] 关键词	文件处理 自托管
[image] 关联	[image]对文件中的敏感数据匿名化
[image] 创建时间	2025年9月10日
[image] **Description**	工具

ConvertX 是一款自托管的在线文件转换器，支持上千种格式，使用TypeScript、Bun和Elysia开发。

主要功能包括文件转换、同时处理多个文件、密码保护和多账户管理。

该转换器支持多种格式，如 JPEG XL、SVG、HEIF、LaTeX、电子书和视频以及矢量图像。

在设置中，您可以使用环境变量控制访问、用户注册和删除旧文件。

 https://github.com/C4illin/ConvertX

[image]
[image]

做移动设备取证和数字调查的开源平台

[image] 关键词	取证 威胁响应 移动设备 自助
[image] 创建时间	2025年9月12日
[image] **Description**	工具

PiRogue 工具套件 - 是一个用于移动设备取证和数字调查的开源平台。该平台由分析工具、知识管理、事件响应管理、证据保存等功能组成，旨在为资源匮乏的民间社会组织提供必要的工具，如数字权利捍卫者、研究人员、记者等。

 https://pts-project.org/

[image]
[image]

开源、离网、去中心化的网状网络

[image]	关键词	传输安全 加密 离线 移动设备 网状网络
[image]	关联	[image]在不安全渠道上尽可能安全地共享秘密 ；[image]安全的秘密共享 ；[image]点对点文件传输 ；[image]在不同操作系统之间传输文件 ；[image]一些私密安全的文件传输解决方案 ；[image]在任何聊天工具中发送算对端加密信息 ；[image]安全共享 ；
[image]	创建时间	2025年9月15日
[image]	**Description**	工具

Meshstatic 是允许用户使用廉价设备构建网状网络并交换加密消息的技术。

如何工作：

- 私人消息使用非对称加密技术进行加密，并在每个用户设备上生成唯一密钥；
- 在群聊中使用 AES-256 加密；
- 在公共频道中，消息也使用 AES-256 加密，但默认情况下，所有 Meshstatic 设备使用相同的预设密码；

哪些设备适用：

- Heltec MeshPocket

- 任何带内置键盘和蓝牙发射器的独立设备；

- 专用Meshstatic调制解调器；

- 由不同电路板、天线和电池组成的DIY套件；

 https://meshtastic.org/docs/introduction/
 https://heltec.org/project/meshpocket/

[image]
[image]

生存训练

[image]	关键词	AI 生存训练 自助
[image]	创建时间	2025年9月16日
[image]	**Description**	工具

Survival AI - The Ark —— 一款专为生存训练设计的聊天机器人，无需网络即可运行.

——帮助在野外寻找并净化水源；

——协助搭建各类庇护设施；

—— 在复杂地形中提供导航；

—— 提供医疗建议；

—— 在停电或其他紧急情况下提供指导；

该产品目前尚不完善，正处于积极开发阶段。

 https://apps.apple.com/us/app/survival-ai-the-ark/id6746391165

适用于iOS和Mac用户。

[image]
☂

智能眼镜隐私保护

[image] 关键词	AI 生物识别 自卫
[image] 关联	[image]当你手握真相：最基本的防护知识
[image] 创建时间	2025年9月17日
[image] **Description**	工具

Privacy Protector for Smart Glasses 是一款实时保护个人信息的工具，适用于智能眼镜的使用场景。

它提供对摄像头视频流的过滤功能，通过模糊或遮盖，对未授权拍摄的人脸进行匿名化处理。

适合敏感行动现场的视觉记录和编辑。

百分百离线。无需云。

https://github.com/PrivacyIsAllYouNeed/protector

[image]
[image]

消除对 Google Web 服务依赖的轻量级方法

[image] 关键词	谷歌 谷歌替代方案
[image] 关联	[image]一些注重隐私的浏览器扩展
[image] 创建时间	2025年9月18日
[image] **Description**	工具

Ungoogled-chromium 是 Google Chromium 浏览器的分支，完全摆脱了对 Google 网络服务的依赖。

该项目旨在提升用户的隐私保护和透明度，提供手动激活功能的选项，以删除剩余的后台请求，删除所有特定于 Google 网络服务的代码。

项目核心目标在于：消除对网络服务的请求、用替代组件替换预装组件，以及禁用削弱用户控制权的功能。

 https://github.com/ungoogled-software/ungoogled-chromium

[image]
[image]

隐写工具

[image] 关键词	传输安全 元数据 加密 隐写术
[image] 关联	[image]一系列隐写工具
[image] 创建时间	2025年9月19日
[image] **Description**	工具

ShadeOfColor 也是一款隐写工具，可将文件隐藏在PNG图像内，从而在数据交换和受限制的情况下提供更高的隐私性。

核心功能包括双向转换、嵌入式元数据、完整性检查、跨平台支持（Windows/Linux/macOS）以及多种加密算法支持。

 https://github.com/archistico/ShadeOfColor2

[image]
[image]

取证工具：磁盘分析和文件恢复

[image] 关键词	取证 对抗性思考方式 数据丢失 自助
[image] 关联	[image]取证和反取证工具及资源
[image] 创建时间	2025年9月23日
[image] Description	工具

Digler是一款用于恢复已删除数据的工具。

该工具支持多种磁盘映像格式，并能独立于文件系统恢复已删除文件。

Digler支持生成DFXML格式的报告，并提供直观的命令行界面。

 https://github.com/ostafen/digler

[image]
[image]

反检测浏览器

[image] 关键词	OSINT 浏览器 网页抓取
[image] 创建时间	2025年9月24日
[image] **Description**	工具

Camoufox是一款开源浏览器，旨在实现可靠的指纹伪装和反机器人系统规避。

它提供广泛的功能，包括智能指纹轮换、地理位置欺骗、以及其他诸多浏览器特征伪装。

兼容最新版本的Firefox。

还能通过光标移动模拟自然用户行为，并具备广告拦截功能。

此外还支持添加自定义字体和隐私设置，例如修改屏幕属性和HTTP参数。

 https://github.com/daijro/camoufox

[image]
[image]

更安全的密码管理解决方案

[image]	关键词	PGP 密码
[image]	创建时间	2025年9月26日
[image]	**Description**	工具

Paasword 是一款创新的密码管理解决方案，它使用 GPG 密钥签名，根据输入的文本生成唯一且安全的密码。

此工具提供高级别的安全性和不可预测性，支持时间伪造功能，可以创建有效期有限的密码。

 https://github.com/biliyoyo520/paasword?tab=readme-ov-file#english-version

[image]
[image]

隐匿点/安全屋周围Wi-Fi入侵检测系统

[image] 关键词	Wi-Fi 威胁识别 安全屋 独居 网络攻击 自检 防御 预防性
[image] 关联	[image]少即是多：变得难以被追踪的简单方法 S03E05
[image] 创建时间	2025年9月30日
[image] **Description**	工具

Air-Guard 是一款实时无线数据监测和分析工具，它使用 ESP32 微控制器实时捕获 WiFi 数据包，并提供图形界面易于使用，以及实时的统计和可视化。

其功括检测 WiFi 网络中的取消认证攻击和 Evil Twin攻击等，以及基于机器学习的 Kr00k 漏洞和网络欺骗攻击检测。

此外，Air-Guard 还会维护日志，并允许您以 .pcap 或 .log 格式导出数据。

 https://github.com/razvan-radutoiu/Air-Guard

[image]
[image]

隐私型浏览器 - 谷歌浏览器替代品

[image] 关键词	数字卫生 数字足迹 浏览器 谷歌替代方案
[image] 关联	[image]消除对 Google Web 服务依赖的轻量级方法 ；[image]隐私型浏览器 - 谷歌浏览器替代品 ；[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御 ；[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式 ；[image]清扫和清点-信息篡改的重要步骤：完美隐身 S04E05 ；[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A ；[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09 ；
[image] 创建时间	2025年10月5日
[image] **Description**	工具

Helium 是一款基于 ungoogled Chromium 的浏览器，注重隐私、广告拦截和极简主义。

与 ungoogled Chromium 不同，它专注于提供更便捷的开箱即用体验，性能和安全性均有所提升，并支持从 Chrome 网上应用店直接安装扩展程序。

适用于所有主要系统，开源。

□ https://github.com/imputnet/helium

[image]
□

洋葱网站模版

[image] 关键词	暗网
[image] 关联	[image]洋葱路由功能的安全信息传递系统
[image] 创建时间	2025年10月6日
[image] **Description**	工具

Onion SSR Boilerplate 是一款注重隐私的 .onion 网站构建模板，提供100% 服务器端渲染 (SSR)，无需客户端JavaScript。这对 Tor 用户尤其有用。

该模板与 Supabase 集成，可通过 REST API 访问数据库。

它还支持通过服务器端验证进行表单处理，以及通过 Docker 部署。

□ https://github.com/profullstack/onion-ssr-boilerplate

[image]
□

2025最新的洋葱链接目录

[image] 关键词	tor 洋葱
[image] 关联	[image]完全Tor
[image] 创建时间	2025年10月7日
[image] Description	工具

暗网资源中心是一个更新的 .onion 链接目录，截至 2025 年。

对于那些想从明网 (clearnet) 搜索 Tor 网站的人，请返回这里：[image]从明网搜索 Tor

□ https://user69blood.github.io/tor-links/

□ 额外福利：https://tor.taxi/

[image]
🔎

与可信赖的朋友安全地共享位置

[image] 关键词	团队 定位 端对端加密
[image] 关联	[image]一些可以欺骗智能手机上的地理位置数据的工具
[image] 创建时间	2025年10月8日
[image] **Description**	工具

Grid Mobile 是一款基于 Flutter 构建的安全位置共享应用，采用端到端加密技术并集成了 Matrix 协议。

该应用帮助您与可信的联系人共享您的位置。跨平台，可在 Android 和 iOS 系统上运行。

主要功能包括实时位置共享、访问控制以及服务器自托管功能。

 https://github.com/Rezivure/Grid-Mobile

[image]

文件转换器 - 开源、完全本地化不用云，永久免费

[image]	关键词	文件处理
[image]	关联	[image]自托管文件转换
[image]	创建时间	2025年10月9日
[image]	**Description**	工具

VERT是一款基于WebAssembly运行的文件转换工具，支持本地化处理无需云端解决方案。

该程序兼容多种格式且无文件大小限制，为用户提供便捷的操作界面。

https://github.com/VERT-sh/VERT

#tools

[image]
[image]

戴面具的电邮

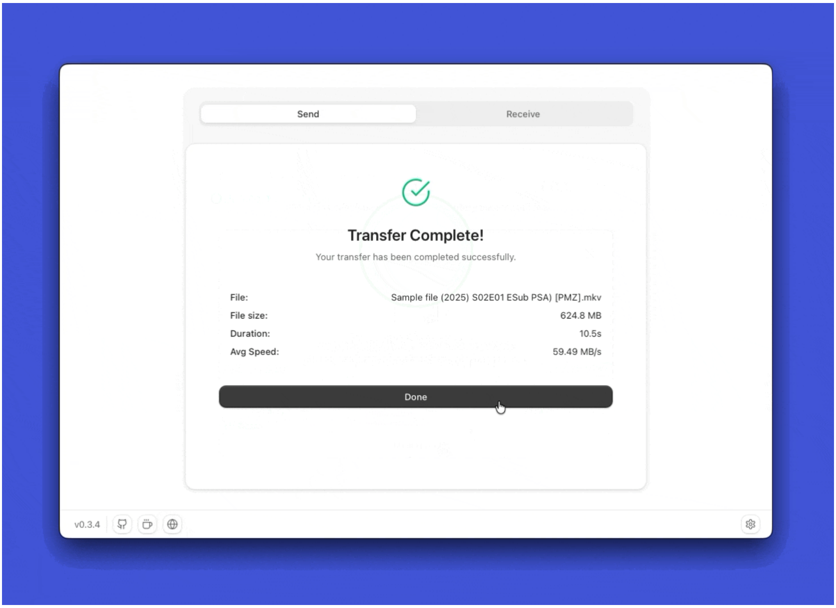
[image]	关键词	免追踪 电邮
[image]	关联	检查可疑电子邮件、链接和文件的在线工具 ；[image]Tor上的加密邮件服务 ；[image]移除你的绵羊墙：给普通人的5个防御课程 ；[image]成为自己的邮件服务提供商 ；[image]一些较安全的电邮客户端选项 ；[image]自我人肉 ；[image]袜子木偶 - 分身创建的小技巧
[image]	创建时间	2025年10月10日
[image]	**Description**	工具

Maildrop 是一款可自行托管且易于使用的临时电子邮件服务，允许在您的域名下接收随机电子邮件地址的邮件。

这款工具非常适合在注册网站时保护您的主邮箱地址隐私。

它还提供创建安全邮箱和自定义邮箱地址的功能。

https://github.com/haileyydev/maildrop/



[image]

点对点文件传输

[image]	关键词	传输安全 加密 数据安全
[image]	关联	[image]安全文件存储 ；[image]取证工具：磁盘分析和文件恢复 ；[image]加密、生成校验和销毁文件 ；[image]云存储文件管理 ；[image]安全地隐藏和加密文件 ；[image]在不同操作系统之间传输文件 ；[image]恢复被删除的文件
[image]	创建时间	2025年10月13日
[image]	**Description**	工具

AltSendme 是一款免费文件传输软件，它使用点对点网络直接在设备

之间传输数据，无需将信息存储在云服务器上。

该程序使用加密技术保护个人数据，且无需注册，从而增强了隐私性。

主要功能包括：支持任意大小和格式的文件传输，并进行完整性检查；自动恢复中断的下载；传输快；以及借助 NAT 支持实现安全、低延迟的连接。

该应用程序适用于 Windows、macOS 和 Linux 系统，具有多语言界面，并为开发者提供命令行支持。

 https://github.com/tonyantony300/alt-sendme/

[image]
[image]

离线安全存储 - 完全本地无需服务器

[image] 关键词	存储安全 数据安全 查询整理 离线
[image] 关联	[image]离线安全传输 ；[image]通过临时Wi-Fi 在设备间离线传输文件
[image] 创建时间	2025年10月14日
[image] **Description**	工具

Savr 是一款用于离线保存在线内容的应用程序，它将数据存储在用户设备本地，实现数据分散化。

无需注册，授权和跨设备同步是可选的（使用您的 Dropbox 或 Google 云端硬盘）。

该应用支持跨平台，可在移动设备和桌面设备上运行。

未来计划推出更多功能，例如图像同步和改进的媒体处理等。

 https://github.com/jonocodes/savr/

[image]
[image]

网状网络通信，支持LoRa 设备

[image] 关键词	IMs 加密 离线 网状网络 通信
[image] 关联	[image]离线安全存储 - 完全本地无需服务器 ；[image]离线安全传输 ；[image]带有频道功能的离线P2P安全通信 ；[image]开源点对点社交网络 ；[image]断网后通信：把智能手机变成“对讲机” ；
[image] 创建时间	2025年10月15日
[image] **Description**	工具

Reticulum MeshChat 是一款网状网络通信应用，支持通过本地网络和互联网发送消息、文件和进行语音通话，并支持通过 LoRa 无线电设备进行通信。

该应用提供安全的数据交换，并兼容 LXMF 客户端。

每个用户都可以创建自己的身份进行匿名通信，并可以使用本地数据库管理消息。

 https://github.com/liamcottle/reticulum-meshchat/

[image]
[image]

2025 年 Tor 使用指南

[image] 关键词	tor
[image] 关联	[image]完全Tor
[image] 创建时间	2025年10月16日
[image] **Description**	工具

1. toriptables2 (https://github.com/ruped24/toriptables2) —— 一个 Linux 实用程序，通过iptables 将所有网络流量重定向到 Tor；

1. tor-ip-changer (https://github.com/seevik2580/tor-ip-changer) — 一个 Python 脚本，定期通过 Tor 请求新的身份；

1. Dark Syenite (https://github.com/CruelDev69/onion-link-validator) — 一个简单的 Python 工具，用于检查 .onion 链接的有效性；

1. Tor Portable (https://github.com/Verity-Freedom/Tor-Portable) — Tor 内核和配置文件的便携版本，支持中文；

1. Tor Bridges Proxy (https://github.com/zerolabnet/tor-bridges-proxy) — 一个极简版 Tor 镜像，包含 SOCKS 5 代理服务器、TorDNS 和一个用于添加桥接的授权 Web 界面；

1. tor-controller (https://github.com/bugfest/tor-controller) —— 用于管理 Kubernetes 集群中的Tor实例和隐藏服务的工

具；

1. TorghostNG (https://github.com/Zopolis4/TorghostNG) —— 类似TorGhost/torguard的工具，将所有流量重定向至Tor，并自动防止DNS泄露；

1. oniongen-go (https://github.com/rdkr/oniongen-go) —— 基于Go语言的超高速.onion（v3）自定义地址生成器，远快于传统python解决方案。

[image]
[image]

本地密码管理器

[image] 关键词	加密 密码 离线
[image] 关联	[image]什么是凭据填充攻击？如何选择密码管理器？
[image] 创建时间	2025年10月17日
[image] **Description**	工具

PearPass 是一款由 Tether 开发的密码管理器，它将凭据完全存储在用户设备上，无需使用云。

设备间P2P同步。可离线使用。

Tether 的 CEO 表示，PearPass 消除了“单点故障”，没有后门，并且可以防止外部篡改或数据泄露。（这话您听听就行）

该应用架构的安全性已获得 Secfault Security 验证。

该应用现已在所有主流平台上提供免费下载。

语言：JavaScript

 https://github.com/tetherto/pearpass-app-desktop

[image]
[image]

从100多个平台下载视频

[image] 关键词	下载
[image] 关联	[image]免费下载工具 ；[image]巧妙地隐藏照片和视频 ；[image]安卓下载器：下载音视频文件
[image] 创建时间	2025年11月1日
[image] **Description**	工具

VidBee 是一款免费开源的视频下载工具，支持从包括 YouTube、TikTok 和 Bilibili 在内的 1000 多个平台下载视频。

它提供简洁的界面、批量下载支持以及通过 RSS 源自动下载功能。

该程序支持选择视频格式和字幕、下载单个视频片段以及下载时进行多任务处理。

VidBee 无需服务器即可在本地运行，确保数据隐私。

语言：TypeScript

 https://github.com/nexmoe/VidBee

[image]
[image]

用手机作为电脑麦克风

[image] 关键词	电脑 移动设备
[image] 关联	[image]户外无设备对话
[image] 创建时间	2025年11月2日
[image] **Description**	工具

AndroidMic - 这款应用可让您将 Android 智能手机用作电脑麦克风。

它支持多种平台，包括 Linux、Windows 和 macOS，并提供 Wi-Fi 和 USB 连接。

主要功能包括降噪、声波可视化和高级音频设置。

语言：Rust

 https://github.com/teamclouday/AndroidMic

[image]
[image]

跨平台AI翻译

[image] 关键词	AI 翻译
[image] 关联	[image]实时语音翻译 ；[image]一系列免费的人工智能翻译器 ；[image]建立国际团结：全球斗争中的人际关系 ；[image]翻译视频
[image] 创建时间	2025年11月3日
[image] **Description**	工具

Prism 是一款基于人工智能的跨平台机器翻译软件。

该程序支持多种操作系统，包括 Windows、macOS 和 Linux。

直观的界面，方便各类用户使用。

语言：Vue

 https://github.com/qyzhg/prism

[image]
[image]

无云自托管文件存储

[image]	关键词	存储安全 文件处理 端对端加密 自托管
[image]	关联	[image]安全文件存储 ；[image]加密、生成校验和销毁文件 ；[image]备份和恢复已删除的文件
[image]	创建时间	2025年11月4日
[image]	**Description**	工具

DriveLite 是一个模块化的、自托管的文件存储平台，提供端到端加密，让用户完全掌控自己的数据。

该平台支持跨设备数据同步，无需依赖第三方云服务。

DriveLite 的设计以易用性和安装便捷性为核心。

语言：TypeScript

 https://github.com/DriveLite/DriveLite

[image]
[image]

互助抗镇压

[image]	关键词	ICE 互助 反监视 突袭 自卫 镇压
[image]	关联	； ； ；
[image]	创建时间	2025年11月20日
[image]	**Description**	工具

推荐使用 ICEOUT - 一种社区警报工具，用于报告ICE 出没的情况。

人们共享实时信息，使他人能够及时了解动态，避免意外遭遇，通过互助支持在ICE行动期间保护彼此。

支持正体简体中文。

类似工具也可用于防御各种突袭、镇压围困、隐蔽监视行动等等危险状况。

□ https://iceout.org/en/

[image]

返回：[image]突袭应对措施

返回：自卫措施

[image]
[image]

从普通浏览器进入Tor网络

[image] 关键词	tor 浏览器
[image] 关联	[image]2025 年 Tor 使用指南; 2025最新的洋葱链接目录;[image]适用于移动设备的Tor浏览器精选;[image]完全Tor
[image] 创建时间	2026年2月27日
[image] **Description**	工具

onion.run 是一个访问暗网网站的入口，让您能够通过普通浏览器访问 Tor 隐藏服务。

支持 Chrome、Firefox、Safari 等浏览器，并兼容超过 100 种浏览器分支。

无需安装、无需配置 —— 只需在任何 .onion URL 后添加 .run 即可安全浏览。

https://onion.run/

[image]

读书和书籍管理，配AI翻译

[image] 关键词	AI 书 查询整理 翻译
[image] 关联	[image]一系列免费的人工智能翻译器 ；[image]一些可选的翻译服务 ；[image]免费读书
[image] 创建时间	2026年4月23日
[image] **Description**	工具

Koodo Reader - 是一款集电子书管理和阅读功能于一体的现代化软件，支持同步和备份，适用于 Windows、macOS、Linux、Android、iOS 及网页平台。

该程序支持 15 种以上的流行电子书格式，包括 EPUB、PDF、MOBI、 AZW3、TXT以及漫画，为您提供灵活多样的阅读来源选择。

核心功能包括：通过 OneDrive、Google Drive、Dropbox 等云服务同步书库、阅读进度、书签、书架、标注和笔记。

Koodo Reader 提供 AI 智能翻译工具、海量词典和内容丰富的注释，以及可自定义的界面，支持更改字体、主题和显示模式。

有中文版。

语言：JavaScript

https://github.com/koodo-reader/koodo-reader

[image]
[image]

“干净”的浏览器

[image] 关键词	免追踪 浏览器 自主
[image] 关联	[image]隐私型浏览器 - 谷歌浏览器替代品 ；[image]适用于移动设备的Tor浏览器精选
[image] 创建时间	2026年4月27日
[image] **Description**	工具

Just the Browser 是一款用于清理浏览器中与网页浏览无关的不必要功能的工具包。

该项目提供脚本，用于重新配置 Google Chrome、Microsoft Edge 和 Mozilla Firefox，禁用那些经常令用户感到厌烦的功能，例如 AI 服务、第三方产品集成、发送遥测数据、以及在新标签页上显示推荐内容等。

该工具包可以移除：

— 所有与 AI 功能相关的内容；

— 购物功能；、

— 赞助内容；

— 所有类型的广告内容；

— 首次启动时显示的请求；

— 所有与收集和发送遥测数据相关的内容 ……

https://justthebrowser.com/

[image]
[image]

一个适用于 macOS 的反取证应用

[image] 关键词	USB 反取证 数据保护 电脑
[image] 关联	[image]免费的macOS清洁软件 ；[image]如何检查MacOS上的恶意软件和键盘监听程序 ；[image]在 Docker 中运行 macOS虚拟机
[image] 创建时间	2026年4月28日
[image] **Description**	工具

swiftGuard - 是一款适用于 macOS 的反取证应用程序，旨在通过监控 USB 端口来保护系统。

该程序会监控 USB 设备的连接和断开，并在发生任何变化时通知用户，必要时还会启动系统关机或睡眠 —— 因为警察会使用鼠标抖动器来阻止屏保和睡眠。

它还允许您将指定设备加入白名单、选择要执行的操作、设置倒计时等。

它在后台运行，并通过系统托盘图标提供有关已连接设备的信息。

语言：Python

https://github.com/Lennolium/swiftGuard

[image]
[image]

看看自己在警察眼里长啥样：浏览器数据的取证分析工具

[image] 关键词	对抗性思考方式 数字取证 浏览器自检
[image] 关联	[image]隐私型浏览器 - 谷歌浏览器替代品 ；[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御 ；[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式 ；[image]清扫和清点-信息篡改的重要步骤：完美隐身 S04E05 ；[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A ；[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09 ；
[image] 创建时间	2026年4月29日
[image] **Description**	工具

ForensiX 是一款用于 Google Chrome 浏览器数据的取证分析工具。

它允许您以只读模式挂载包含 Chrome 数据的卷，从而确保数据完整性并执行哈希验证。

主要功能包括：嫌疑人画像和行为评估（包括个人信息、Chrome 元数据和目标系统元数据）；使用机器学习模型对浏览历史记录 URL 进行分类；以及按时间段分析凭据使用频率和浏览活动。

ForensiX 还提供访问时长、自动填充数据、下载、书签、网站图标、缓存和卷结构等信息，并维护一个共享数据库，用于保存调查人员发现的潜在证据。

语言：JavaScript

 https://github.com/ChmaraX/forensix

[image]
[image]

找信号：对抗黄貂鱼等监视设备

[image]	关键词	Wi-Fi 自卫 蓝牙 黄貂鱼
[image]	关联	[image]黄貂鱼
[image]	创建时间	2026年5月8日
[image]	**Description**	工具

Wigle App - 是一款可绘制 Wi-Fi 和蓝牙信号分布图的移动应用。

活动家和研究人员可利用这些地图识别与监控设备、执法装置或固定监测点相关的信号模式。

 https://wigle.net/

[image]
[image]

免 KYC 的交易平台（精选）

[image] 关键词	加密货币 匿名 身份验证
[image] 关联	[image]调查区块链上的交易；[image]绕开KYC 的情况下用加密货币交换加密货币的方法；[image]隐私堡垒门罗币 - 服务清单2026：钱包、交易所、匿名SIM卡、主机及其他
[image] 创建时间	2026年5月13日
[image] **Description**	工具

1. eigenwallet (https://eigenwallet.org/) — UnstoppableSwap 的新版本，支持比特币到门罗币的原子互换；

2. retoswap (https://retoswap.com/) — 基于 Haveno、Tor 和门罗币构建的私密、非托管 P2P 平台；

3. XmrBazaar (https://xmrbazaar.com/) — 小众圈内知名的门罗币 P2P 交易市场；

4. CypherGoat (https://cyphergoat.com/) — 提供丰富交易对的加密货币交易所；

5. BitBridge (@bit_bridge_bot) — Telegram上另一个小众知名的兑换平台。

[image]
[image]

基于人工智能的暗网开源情报工具

[image] 关键词	AI 开源情报 暗网
[image] 关联	[image]Tor工具系列 ；基于人工智能的暗网开源情报工具 ；您的专业级私人情报终端已开源 ；跨平台社交媒体情报 - 追踪和自检 ；监视资本主义之外的元搜索引擎 ；[image]开源情报工具库2026
[image] 创建时间	2026年5月14日
[image] **Description**	工具

robin - 是一个利用AI在暗网进行开源情报研究的工具。

它使用大型语言模型进行查询、过滤搜索结果、并提供调查摘要。

可自动访问多个暗网搜索引擎和洋葱网站索引，收集并解析找到的暗网页面，忽略掉失效的链接和噪音，并将收集到的内容通过LLM进行处理，以清理、构建和总结结果，满足分析人员的需求。

该程序支持多种AI模型，并采用模块化架构以提高灵活性。

语言：Python

 https://github.com/apurvsinghgautam/robin

[image]
[image]

从数据库中自动生成美观易读的ER图（给本项目二期工程培训基地参考）

[image] 关键词	实体关系图 数据处理 数据库
[image] 创建时间	2026年5月15日
[image] **Description**	工具

Liam ERD 是一款能够根据数据库自动创建美观易读的实体关系图的工具 —— ERD：一种展示系统中实体及其相互关系的图形化图表。

它提供交互式用户界面，支持平移、缩放和筛选功能，让您轻松理解复杂的图表。

Liam ERD 针对各种规模的项目进行了优化，能够高效处理超过 100 个图表。

语言：TypeScript

 https://github.com/liam-hq/liam

[image]
[image]

翻译视频

[image] 关键词	AI 翻译 语音识别
[image] 关联	[image]一些可选的翻译服务；[image]一系列免费的人工智能翻译器；[image]跨平台AI翻译；[image]实时语音翻译
[image] 创建时间	2026年5月22日
[image] Description	工具

Linly-Dubbing - 是一个开源工具，利用人工智能技术自动将视频翻译成多种语言。

它支持自动视频上传、人声分离、语音识别、基于大型语言模型的翻译以及语音合成。

它集成了多种技术，例如用于视频上传的 yt-dlp、用于人声分离的 Demucs 和 UVR5、用于语音识别的 WhisperX 和 FunASR，以及用于翻译的 OpenAI API 和 Qwen。

语音合成采用 Edge TTS、XTTS、CosyVoice 和 GPT-SoVITS，提供高质量的配音。

它还支持与数字虚拟形象进行唇形同步，增强翻译内容的真实感。

语言：Jupyter Notebook

□ https://github.com/Kedreamix/Linly-Dubbing

[image]
[image]

清除电脑上的取证痕迹

[image] 关键词	数字取证 电脑 自检 预防性
[image] 关联	[image]计算机取证 ；[image]取证工具：磁盘分析和文件恢复 ；[image]恢复被删除的文件
[image] 创建时间	2026年5月25日
[image] **Description**	工具

Nyx 是一个独立的脚本，用来清理 Linux、macOS 和 Windows 系统上的取证痕迹。

它可以删除临时文件、日志和其他可用于恢复已删除信息的痕迹。

跨平台支持，确保无论操作系统如何，都能提供一致的清理效果。

语言：Shell

 https://github.com/evilsocket/nyx

[image]

家庭管理

[image] 关键词	团队 管理 自托管
[image] 关联	[image]在本地运行AI
[image] 创建时间	2026年5月26日
[image] **Description**	工具

HomeHub 是一款轻量级、私密、无需登录、可自行托管的 Web 应用，专为管理家庭生活而设计。

该应用提供共享笔记、云存储、购物清单、任务追踪、带提醒的日历、家庭成员考勤、开销追踪和视听媒体下载器等功能。

所有数据均存储在您的本地网络中，确保完全隐私，无需云服务或进行任何追踪。

该应用拥有直观简单的界面，操作无需技术水平，并支持通过配置文件自定义功能和颜色主题。

语言：HTML

https://github.com/surajverma/homehub

[image]
[image]

3D资源库

[image] 关键词	3D
[image] 创建时间	2026年5月27日
[image] **Description**	工具

awesome-3d-printing 是一个汇集了最佳 3D 打印资源、工具和软件的库。

包含用于创建、编辑和准备 3D 模型的程序链接，以及用于管理打印机的实用程序。

汇集了建模工具、切片软件、打印监控及数据分析的软件。

 https://github.com/ad-si/awesome-3d-printing

[image]
[image]

有人在悄悄监视你吗？

[image] 关键词	个人 反监视 智能眼镜 自卫 街头
[image] 关联	☂智能眼镜隐私保护 ；[image]隐蔽监视 ；[image]反监视 ；[image]“不要再拍了！请关闭设备删除影像”
[image] 创建时间	2026年5月29日
[image] **Description**	工具

yj_nearbyglasses - 这款安卓应用旨在检测附近带有摄像头的智能眼镜，并在检测到此类设备时提醒用户。

它会扫描周围区域，查找被识别为智能眼镜的设备，并在检测到时通知用户。

该应用有助于保护用户隐私，提醒用户注意可能利用此类设备进行的隐蔽视频监控。

日志仅记录在本地，不会自动与任何人共享。日志中几乎不包含敏感数据。

语言：Kotlin

 https://github.com/yjeanrenaud/yj_nearbyglasses

[image]
[image]

文件上传恶意软件扫描

[image] 关键词	恶意软件 数据安全 病毒检测 自检
[image] 关联	[image]安卓恶意软件扫描器 ； 恶意软件
[image] 创建时间	2026年6月2日
[image] **Description**	工具

pompelmi - 是一个类似于 VirusTotal 的免费开源文件扫描工具。

它会在下载过程中扫描已下载的文件，检测是否存在恶意代码，然后再将文件保存到磁盘。

它支持对 ZIP 压缩包进行深度扫描，并允许您根据文件扩展名、大小和 MIME 类型设置控制策略。

该工具兼容 Express、Koa 和 Next.js 框架，并提供相应的集成适配器。

语言：TypeScript

 https://github.com/pompelmi/pompelmi

[image]
[image]

自托管黑头套紧急响应

[image] 关键词	个人 威胁响应 强迫失踪 自助 预防性
[image] 关联	[image]预防‘黑头套’；[image]为孤军奋战者准备的预警方案；[image]藏匿点或安全屋；[image]S01E01-T2 识别威胁并作出反应；[image]抢先采取行动 - 反侦基础课 S06E01：七点规则和态势感知
[image] 创建时间	2026年6月8日
[image] **Description**	工具

LastSignal 也是一个防黑头套的“自杀程序”，开源、自托管。

它允许用户创建端到端加密的消息，当所有者停止按照指定时间以方式打卡报平安时，预制的消息会自动发送给可靠的收件人。

该功能适用于在突发失联（即强迫失踪/暗杀/秘密逮捕）时传递重要信息，例如资金管理权限、正义事业接棒权限、或私人文件。

所有加密操作（采用XChaCha20-Poly1305和Argon2id算法）均在用户浏览器端完成，数据上传至服务器前已完成加密，因此即使托管软件本身也无法读取消息内容。

部署方式简单 —— 通过Docker在任意配备SMTP服务器的SSH上运行； 支持灵活的检查计划、基于恢复码的紧急停止及完整操作审计。

□ https://github.com/giovantenne/lastsignal

[image]
[image]

Veilid 网络上的匿名私密通信工具

[image] 关键词	IMs P2P Veilid 匿名 团队
[image] 关联	离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线**P2P**安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机” ；[image]网状网络通信，支持LoRa 设备
[image] 创建时间	2026年6月9日
[image] **Description**	工具

VeilidChat 是一款实验性的私密通讯工具，旨在演示 Veilid 网络。

它本质上和 Signal 或 Ricochet 类似，不同的是它运行在全新的匿名 **P2P** 网络 **Veilid** 上。

- 端到端消息加密；
- 去中心化网络；
- 匿名消息路由；
- 无需手机号码或邮箱；

VeilidChat 基于 Veilid 协议构建，该协议融合了 Tor、DHT/P2P 网络和加密密钥认证的理念。

Veilid 超越现有的隐私技术，并有可能彻底改变人们使用互联网的方式。**Veilid**没有盈利动机，能够在不妥协于资本主义的前提下以独特的方式推广隐私安全理念。

 https://github.com/kyanha/veilidchat?tab=readme-ov-file

[image]
[image]

监视资本主义之外的元搜索引擎

[image] 关键词	元搜索引擎 开源情报 自托管 隐私
[image] 关联	[image]隐私自助：流行产品的开源替代品目录 ；[image]Tor工具系列
[image] 创建时间	2026年6月10日
[image] **Description**	工具

SearXNG - 是一个免费的互联网元搜索引擎，它聚合了来自各种搜索服务和数据库的结果。用户既不被跟踪，也不被剖析。

安全、加密的连接，支持自托管，支持243个搜索引擎，其中89个是默认启用的；58个语种的翻译，大约70个维护良好的实例。以及其他特色。

 https://docs.searxng.org

[image]
[image]

注重隐私的智能手机

[image] 关键词	硬件 移动设备
[image] 关联	[image]如果您的手机被盗了或被警察抢走了，怎么办
[image] 创建时间	2026年6月15日
[image] **Description**	工具

1. Librem 5 —— 最硬核的选择之一。内置三个安全硬件开关。运行PureOS系统。可更换调制解调器，而且是开源的。

2. PinePhone —— 面向极客的模块化手机。运行Linux，可安装postmarketOS、Ubuntu Touch和Manjaro。同样配备硬件安全开关。

3. Punkt MC03—— 运行AphyOS 的新款隐私型智能手机。内置应用沙盒，可能禁用了所有追踪器。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

返回：[image]到底也没有无法被监听的电话？：变得难以被追踪的简单方法 S03E08

当然，如你所知，鉴于移动设备的工作原理它无法保证百分百的隐私和匿名性，但值得注意的是，市场上此类智能手机正在逐渐增多。

最佳方案之一是购买一步智能手机并自行配置。例如使用 Google Pixel ＋ GrapheneOS、或者 Fairphone 5 ＋ /e/OS，以及已经移除 Google 服务的 Pixel 手机并刷入你选择的自定义固件。

以及，至少还需要使用一次性SIM卡、通过Tor路由流量、避免LTE网络、分身隔离账户，以及其他许多需要在实践中逐步掌握的自我保护操作。

[image]

返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

额外推荐：Spirit Phone（内置Raspberry Pi Compute Module 5）

[image]
[image]

隐私安全型开源家庭服务器

[image]	关键词	存储安全 服务器 网络攻击 自主 隐私
[image]	创建时间	2026年6月24日
[image]	**Description**	工具

Cosmos-Server - 是一个安全易用的开源家庭服务器，用户可以在不牺牲安全性和稳定性的前提下，掌控自己的数据并维护隐私。

主要功能包括用户身份验证、抵御 DDoS 和机器人攻击，以及通过直观的 Web 界面管理和部署各种应用程序。

此外，Cosmos-Server 还支持与 RClone 集成，实现远程存储管理，并使用 Restic 提供容器和数据备份和恢复功能。

语言：JavaScript

 https://github.com/azukaar/Cosmos-Server

[image]
[image]

在不安全渠道上尽可能安全地共享秘密

[image] 关键词	传输安全 加密
[image] 关联	[image]安全的秘密共享；[image]点对点文件传输；[image]在不同操作系统之间传输文件；[image]一些私密安全的文件传输解决方案；[image]在任何聊天工具中发送算对端加密信息；[image]安全共享；
[image] 创建时间	2026年6月26日
[image] **Description**	工具

Yopass 是一款用于安全共享密钥、密码和文件的工具，旨在尽可能减少通过电子邮件或即时通讯等不安全渠道传递敏感信息的风险。

它使用 OpenPGP 提供端到端加密，确保服务器永远不会访问未加密的数据。

消息可以配置为一次性查看（之后自动删除）或生命周期（到期后自动销毁）。

Yopass 无需创建帐户或用户管理，简化了共享流程。

语言：TypeScript

https://github.com/jhaals/yopass

[image]
[image]

隐私堡垒门罗币 - 服务清单 2026：钱包、交易所、匿名SIM卡、主机及其他

[image] 关键词	SIM匿名 加密货币 自托管 门罗币 隐私
[image] 关联	[image]免 KYC 的交易平台（精选）；调查区块链上的交易；绕开**KYC** 的情况下用加密货币交换加密货币的方法
[image] 创建时间	2026年6月29日
[image] **Description**	工具

以下整理了一份服务清单，供珍视并使用门罗币（Monero）的用户参考。

1. 钱包

Monero GUI Wallet（ https://www.getmonero.org/downloads/#gui)——门罗币官方桌面钱包。

Feather（ https://featherwallet.org/ ）— 轻量且极简的官方钱包替代方案。桌面版。

Cake Wallet（ https://cakewallet.com/ ）— iOS 钱包，支持 BTC、LTC、XMR。

Monerujo (https://www.monerujo.app/) — 面向 Android 用户的 XMR 钱包。

Monero One (https://apps.apple.com/us/app/monero-one/id6757898541) — 面向 iOS 用户的全新非托管型 XMR 移动钱包。

2. 交易所和服务

XmrBazaar (https://xmrbazaar.com/)— 小众圈内颇具知名度的点对点市场，除XMR币外，还可购买全球范围内的各类商品和服务。

eigenwallet (https://eigenwallet.org/) — UnstoppableSwap的新版本，支持比特币和门罗币的原子交换。

3. 匿名SIM卡/短信服务

simsup (https://simsup.net/) — 面向全球销售匿名SIM卡的服务。支持XMR/BTC支付。

sms4sats (https://sms4sats.com/) — 热门短信接收服务。

crypton (https://crypton.sh/) — 提供匿名SIM卡的服务。

JMP (https://jmp.chat/) — 通过XMPP发送短信和拨打电话的服务。

monerosms (https://monerosms.com/) — 发送匿名短信的服务，支持XMR支付。

4. 支持XMR支付的主机服务

njalla (https://njal.la/)

Privex (https://www.privex.io/)

MyNymBox (https://mynymbox.io/)

1984 Hosting (https://1984.hosting/)

NiceVPS (https://nicevps.net/)

IncogNET (https://incognet.io/)

额外：

Monerica (https://monerica.com/) — 整合各类使用XMR作为支付手段的服务与商家的聚合平台。

[image]
[image]

离线知识库：应对灾难和突发状况

[image] 关键词	AI 存储安全 战争 气候灾难 离线 自助 预防性
[image] 关联	离线安全存储 - 完全本地无需服务器 ；离线安全传输 ；带有频道功能的离线P2P安全通信 ；开源点对点社交网络 ；断网后通信：把智能手机变成“对讲机”
[image] 创建时间	2026年7月6日
[image] **Description**	工具

一个集AI、维基信息库、地图、医学参考资料和完整教育课程于一体的独立离线服务器。

无需网络。无需云。无需订阅。即开即用。

包括以下功能：

→ 由Ollama驱动的本地AI助手（完全离线运行）

→ 完整的维基百科内容，可下载并支持搜索

→ 任意地区的离线地图

→ 医学参考资料和生存指南等

→ 带学习进度追踪的完整可汗学院课程

→ 通过CyberChef提供的加密与数据分析工具

→ 支持语义搜索的文档上传功能（本地RAG）

还有更多。

只需要：一块太阳能板、一块电池、一台小电脑和一个WiFi接入点。仅此而已。即可实现完整的离网知识站。功率范围15至65瓦。无论是在木屋、房车、帆船还是地堡中都能使用。

只需一条命令即可安装。

100%开源。Apache 2.0许可证。

 https://github.com/Crosstalk-Solutions/project-nomad

[image]
[image]

跨平台社交媒体情报 - 追踪和自检

[image] 关键词	个人 团队 对抗性思考方式 开源情报 数字足迹 独立调查 社交媒体情报 自检 防御
[image] 关联	分身 ；[image]数字技术限制和最佳实践 ；[image]镇压应对措施
[image] 创建时间	2026年7月7日
[image] **Description**	工具

Tookie 是一款高级开源情报工具，旨在根据输入的数据搜索社交媒体帐户。

支持跨平台，可以对目标用户的在线活动进行全面分析。

该工具的设计以易用性为核心，对安全专业人员和研究人员都非常有用。

有中文。

语言：Python

 https://github.com/Alfredredbird/tookie-osint

[image]
[image]

暗网调查工具：去匿名化

[image] 关键词	tor 对抗性思考方式 暗网 独立调查 自检 预防性
[image] 关联	[image]数字技术限制和最佳实践 ；[image]使用Tor保护自己时千万不要做这9件事 ；[image]完全Tor ；[image]Tor工具系列 ；[image]适用于移动设备的Tor浏览器精选 ；[image]从明网搜索 Tor ；分身
[image] 创建时间	2026年7月8日
[image] Description	工具

暗网可能并不像您想象中那么匿名。有人开发了一种工具，可以剥去隐藏站点的面具。它叫OnionScan。

只需一个命令。指向任何 .onion 暗网站点，它就会扫描该该站的每个角落，告诉你它有多匿名。

你会发现它们中大多数都没那么匿名。

以下是 OnionScan 自动发现的东西：

→ 配置错误导致泄漏的真实 IP 地址；

→ 忘记清除的GPS 坐标隐藏在图像元数据中，揭示了照片拍摄的位置；

→ 与明网服务器匹配的SSH指纹，暴露了真实位置；

→ 软件版本和服务器横幅，精确识别具体机器；

→ SMTP 和 FTP 网站横幅泄露了主机名称和操作系统版本；

→ 站点之间的相关性 —— 表明它们由同一个人运行；

→ 比特币地址、电邮地址和 PGP密钥，都可将身份联系起来...

OnionScan 还拥有关联实验室—— 一个网络仪表板，可以映射扫描站点之间的关系，由此挖掘到背后的操作者忽略了的模式问题。比如，同一个 SSH 密钥在两个“看起来不相关”的网站上出现、同一电子邮件、同一服务器 …… 它将这些线索点连接起来。

本工具的收入一如既往用于自检和独立调查。

 https://github.com/s-rah/onionscan

[image]

返回：[image]数字技术限制和最佳实践

返回：分身

[image]
[image]

您的专业级私人情报终端已开源

[image] 关键词	AI 开源情报 独立调查 自助
[image] 关联	[image]跨平台社交媒体情报 - 追踪和自检 ；基于人工智能的暗网开源情报工具 ；您的专业级私人情报终端已开源 ；监视资本主义之外的元搜索引擎
[image] 创建时间	2026年7月9日
[image] **Description**	工具

您的私人情报终端 Crucix 已开源。

它可以实时监控全球27个数据源，一旦有动态就会向你发出提醒。

政府和情报机构为此类系统支付的费用高达六位数。而这款工具能在您的笔记本电脑上免费运行。

无需云。无需订阅。没有遥测。也无需安全许可。所有数据均开放，在您自己的机器上进行聚合和交叉关联，每 **15** 分钟更新一次。

监测的内容包括：

→ ACLED：全球武装冲突事件

→ 通过 FRED 获取美联储经济指标

→ OFAC + OpenSanctions：制裁筛查

→ 17 个精选的 Telegram 情报频道，用于社交舆论监测

→ 海事AIS：船舶追踪和制裁规避检测

→ GDELT：覆盖100多种语言的全球事件追踪

→ 世界卫生组织（WHO）：疾病爆发预警

→ ReliefWeb：联合国人道主义数据

→ CelesTrak：国际空间站（ISS）、星链、OneWeb

→ VIX指数和信用利差风险指标

每次扫描都会计算自上一个周期以来，哪些情况发生了变化、哪些事态升级、哪些事态缓和。

接入大语言模型（Claude、GPT、Gemini），即可基于跨领域信号关联生成交易策略。即便没有接入大语言模型，确定性规则引擎仍会全面评估所有数据。

18个以上数据源无需API密钥即可使用。设置过程简单便捷。

100%开源。MIT许可证。

🔗 https://github.com/calesthio/Crucix

[image]
[image]

新闻收割机

[image]	关键词	AI 新闻 生产力
[image]	创建时间	2026年7月15日
[image]	**Description**	工具

ClawFeed 是一款开源工具，旨在自动收集和整理来自各种来源（例如 Twitter、RSS、HackerNews、Reddit 和 GitHub等）的新信息。

它利用人工智能技术过滤并生成结构化报告。报告频率可选：每 4 小时、每天、每周或每月。

ClawFeed 支持“资源打包”，可与社群分享；为内容添加书签，可进行人工智能驱动的深度分析。

可以作为独立应用程序部署，也可以集成到 OpenClaw 和 Zylos 平台中，以实现自动生成摘要和信息流管理。

语言：HTML

 https://github.com/kevinho/clawfeed

[image]
[image]

安全工具箱规整 - 2026版

[image] 关键词	个人 元搜索 加密 安全搜索 工具 查询整理 清理 电脑 病毒检测 离线 移动设备 自卫 防御 预防性 高科技 镇压
[image] 创建时间	2026年7月17日
[image] **Description**	工具

基本款 ——

1. Portmaster 是一款终极应用防火墙和网络监控工具，例如，它能精确显示每个应用的连接位置：

https://safing.io/portmaster

2. SearXNG 允许您自建私有的元搜索引擎，提供媲美谷歌的搜索结果，且完全无追踪： https://searxng.org

3. PrivateBin 是一款加密的自建粘贴板，可确保您的笔记、代码片段等内容保持私密： https://privatebin.info

4. RethinkDNS 是一款集防火墙、DNS 切换器和追踪器拦截器于一体的工具，可增强 Android 系统的隐私保护： https://rethinkdns.com

5. Picocrypt 是一款极其简单且超安全的文件加密工具，它可以创建与随机数据无法区分的加密卷： https://github.com/Picocrypt/Picocrypt

6. NewPipe 是一款注重隐私的 Android YouTube 客户端，无广告、无追踪且支持后台播放： https://newpipe.net

7. OnionShare 支持通过 Tor 进行安全的文件共享和聊天，无需服务器、无需账户： https://onionshare.org

8. Obtainium 可直接从 GitHub 或 F-Droid 自动更新您所有的开源 Android 应用，完全无需应用商店： https://github.com/ImranR98/Obtainium

9. LocalSend 是一款开源的 AirDrop 替代方案，支持极速本地文件共享： https://localsend.org

10. Hypatia - 一款Android 实时恶意软件扫描器，速度极快、使用内存小，完全离线： https://github.com/MaintainTeam/Hypatia

11. Cryptomator - 在文件上传至云端前即对其进行加密，因此云服务提供商无从知晓您上传的是什么： https://cryptomator.org

12. Joplin - 一款完全加密的开源笔记应用，支持端到端加密同步和 Markdown 格式： https://joplinapp.org

[image]
[image]

开源情报工具库2026

[image] 关键词	对抗性思考方式 开源情报 独立调查 自检 防御
[image] 关联	[image]基于人工智能的暗网开源情报工具 ；[image]您的专业级私人情报终端已开源 ；[image]跨平台社交媒体情报 - 追踪和自检 ；[image]监视资本主义之外的元搜索引擎
[image] 创建时间	2026年7月20日
[image] **Description**	工具

这里是一个巨大的工具库，收纳的是用于信息收集、网络安全、反向搜索、漏洞赏金、信任与安全、红队行动等方面的开源情报工具。

百分百免费。

 https://github.com/Astrosp/Awesome-OSINT-For-Everything/

[image]
[image]

离线图像压缩工具

[image] 关键词	离线 管理
[image] 关联	[image]也是隐写：将敏感信息隐藏在图像中
[image] 创建时间	2026年7月23日
[image] **Description**	工具

caesium-app-web - 是一个现代图像压缩 Web 应用，完全离线运行于浏览器中，确保数据隐私。

该应用支持 JPG、PNG、WebP 和 TIFF 图像的压缩，让您在不会显著损失图像质量的情况下减小文件大小。

用户界面直观，使压缩过程快速便捷。

语言：JavaScript

 https://github.com/Lymphatus/caesium-app-web

#tools #图像压缩 #离线

[image]
[image]

随手存档

[image] 关键词	存档 管理
[image] 关联	[image]一个功能强大的自托管 Internet 存档解决方案 ；[image]交互式高质量网页存档
[image] 创建时间	2026年7月24日
[image] **Description**	工具

wayback-machine-webextension - 是互联网档案馆开发的浏览器扩展程序，适用于 Chrome、Firefox、Edge 和 Safari 浏览器，旨在与 Wayback Machine 集成。

它允许您立即将当前网页保存到 Wayback Machine 存档，查看其最早和最新的版本，以及概览所有已保存的副本。

此外，该扩展程序还可以自动检查已访问页面的状态，并为无法访问的网站推荐存档版本。

语言：JavaScript

 https://github.com/internetarchive/wayback-machine-webextension

[image]
[image]

安全的文件存储与共享

[image] 关键词	存储安全 文件处理 查询整理 管理
[image] 关联	[image]文件上传恶意软件扫描 ；[image]安全文件存储 ；[image]加密、生成校验和销毁文件 ；[image]备份和恢复已删除的文件 ；[image]无云自托管文件存储 ；[image]点对点文件传输
[image] 创建时间	2026年7月27日
[image] **Description**	工具

Twake Drive 是一款安全、开源的文件存储解决方案，适合专业用途。

用户可以将文件安全地存储在云端或自己的服务器上，并与合作伙伴和团队共享。

该程序确保隐私和数据安全，提供用户友好的界面，并可与办公应用程序集成。

Twake Drive 支持按文件内容、标题和发件人进行全文搜索，使文档浏览和管理更加便捷。

语言：JavaScript

 https://github.com/linagora/twake-drive

[image]
[image]

自托管AI会议助手

[image]	关键词	AI 会议 组织 自托管
[image]	创建时间	2026年7月31日
[image]	**Description**	工具

Meetily 是一款注重隐私的 AI 会议助手，无需使用云服务即可在本地处理数据。

它提供使用 Parakeet 和 Whisper 模型的实时转录、说话人识别以及使用 Ollama 生成会议摘要的功能。

该程序完全开源，支持自托管，兼容 macOS 和 Windows 系统，并可与 Zoom、Microsoft Teams 和 Google Meet 等多种视频会议平台兼容。

语言：Rust

https://github.com/Zackriya-Solutions/meetily

[image]
[image]

反追踪浏览器

[image] 关键词	反追踪 数字足迹 浏览器
[image] 关联	[image]隐私型浏览器 - 谷歌浏览器替代品 ；[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御 ；[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式 ；[image]清扫和清点-信息篡改的重要步骤：完美隐身 S04E05 ；[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A ；[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09 ；
[image] 创建时间	2026年8月3日
[image] Description	工具

Donut Browser 是一款开源的反追踪浏览器，旨在保障用户在互联网上的匿名性和隐私。

它支持创建无限数量的独立的配置文件，每个配置文件都拥有独特的指纹、Cookie、扩展程序和数据。

该浏览器基于 Chromium 和 Firefox 内核构建，并配备了先进的指纹伪装工具。

Donut Browser 不收集遥测数据，并支持通过云端同步配置文件，且

提供端到端加密选项。

语言：Rust

 https://github.com/zhom/donutbrowser

[image]
[image]

噪声生成式混合网络，比Tor更胜一筹

[image] 关键词	VPN 元数据 加密 反追踪 混合网络
[image] 关联	[image]离线安全存储 - 完全本地无需服务器 ；[image]离线安全传输 ；[image]带有频道功能的离线P2P安全通信 ；[image]开源点对点社交网络 ；[image]断网后通信：把智能手机变成“对讲机” ；[image]网状网络通信，支持 LoRa 设备
[image] 创建时间	2026年8月4日
[image] **Description**	工具

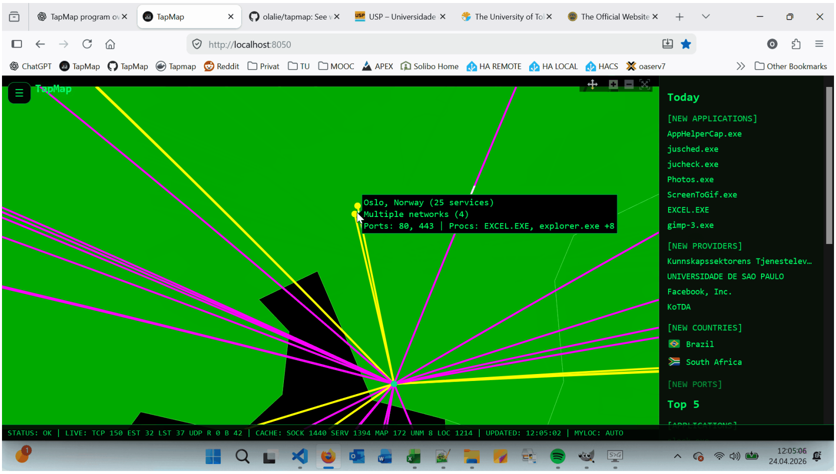
Nym Mixnet 是一个类似于 Tor 的匿名网络，但采用了能更好地隐藏元数据的混合网络（mixnet）架构。

- 于 2026 年 2 月进行了更新；
- 采用 Noise Protocol 和 WireGuard 加密技术；
- 多层加密、流量掩护；
- 采用 5 跳混合网络（Tor 为 3 跳）。

经过此次更新，Nym 网络已迈入匿名网络发展的全新阶段。是目前

市场上唯一能够解决元数据泄露问题的技术。

 https://nym.com/zh-Hans/mixnet



[image]

实时查看您的计算机所连接的位置

[image] 关键词 网络安全 自检

[image] 关联 [image]噪声生成式混合网络，比Tor更胜一筹

[image] 创建时间 2026年8月5日

[image] **Description** 工具

tapmap - 是一个可以实时在交互式世界地图上可视化您的计算机网络连接的工具。

它会显示您的计算机正在连接的地理位置，方便您识别异常或可疑的连接。

可在 Windows、Linux 和 macOS 上本地运行。不收集遥测数据。Linux 系统支持 Docker。

语言：Python

 https://github.com/olalie/tapmap

[image]
[image]

把你的Telegram变成无限云存储

[image] 关键词	telegram 云存储 跨平台
[image] 关联	[image]Telegram内容提取工具 ；[image]Telegram 语音笔记转录和摘要机器人 ；[image]Telegram 探索工具 ；
[image] 创建时间	2026年8月6日
[image] **Description**	工具

Telegram-Drive - 是一款开源的跨平台桌面应用程序，可将您的 Telegram 账户转变为无限容量的云存储空间。

该程序支持上传、下载和整理文件。

采用 Tauri、Rust 和 React 开发，确保高性能、响应迅速。

语言：TypeScript

 https://github.com/caamer20/Telegram-Drive

[image]

威胁知识库-索引页

📍

本知识库一定程度上对 本站点整体 起到了战略性导航的作用。

🎯

简述

本知识库旨在通过帮助您了解镇压当局和统治者的社会控制最可能使用的手段，从而更清晰地呈现激进派行动者需要掌握并提早准备的防御措施。

本数据库可作为前线社区防御工作的标准框架在您的培训工作中采取。

独立学习者可以根据自己和亲密团队的特定威胁模型针对性使用本数据库，并鼓励您以此框架为线索查找到更多更深入地探讨这些主题的材料。

感谢 Notrace 贡献的专业且系统的学习资源。

🔑

对威胁库的特别说明

威胁库作为工具的设计本质上是一种非常技术化的反压迫方法。

威胁建模是在行动层面进行的，因此并不试图解决社会问题 —— 例如如何逃离镇压者所寻求的封锁围困（不论是信息封锁还是经济封锁或其他）、或者如何干预社会紧张局势等等。

争取自由的斗争不仅仅是技术问题，更是社会问题，并且会产生心理和情感影响。我们鼓励您在行动前、行动中和行动后，尽可能与所有参与者进行讨论，并 确保每个人的情感需求得到考虑。

本项目将在未来的《战术》主题站点中对此进行更详细探讨。

威胁库旨在尽可能全面地涵盖无政府主义者和其他反叛行动者可能面临的威胁，并追求与时俱进的更新。安全领域没有长久有效的“标准答案”，这一点尤其正确，因为对手肯定会发展出新的和意想不到的镇压技术。

为了避免使用威胁库有可能带来的虚假安全感，我们鼓励您关注更广泛的知识来源，保持批判性思考，并在做出重要决策时始终考虑您的个人风险评估和适用性。

[image]
☠️

镇压手段

关于我们将要或正在面对的是什么 —— 包括可见的和不可见的镇压手段，其威胁程度不相上下。

☠️镇压手段
[image]
🪖

自卫措施

关于我们可以如何在镇压环境中保护自己，尽可能降低风险。

自卫措施
[image]

带有攻击树的威胁库用例示范

关于如何在生活中、在特定项目中、或在行动时运用威胁库工具的示范。

[image]带有攻击树的威胁库用例示范

[image]
☠️

镇压手段

风险矩阵

👮

威胁

[image]敲门 🐝人肉搜索 🚔增加警力 👀大规模监视

- 4个子项目 💬平民告密 👁️‍🗨️大规模数字监控 [image]警方档案(网格) [image]视频监控

[image]身体暴力(含酷刑) [image]警察巡逻

🚔

指控

[image]对证据的偏见性解读 [image]隐蔽性

地突袭住所 [image]隐蔽的监视设备

- 3个子项目 👂窃听 🔎定位追踪 📹偷拍

[image]警犬 [image]敲门 👎栽赃 [image]法医取证

- 10个子项目 🔥纵火 🔫弹道学 [image]数字取证 🧬DNA 🎭面部识别 [image]指纹 🚶步态识别 ✍笔迹分析 [image]语言指纹 🪶痕量证据鉴定

🏚抄家 🕵身份检查 👹渗透者 🐀告密者（线人） 🌎跨国维稳 🩺审讯心理学 👀大规模监视

- 4个子项目 💬平民告密 👁🗨大规模数字监控 [image]警方档案(网格) [image]视频监控

🕸网络映射 🔍开源情报 🚿刑侦证据洗白 [image]物理监控（上岗）

- 3个子项目 🚁空中监视 [image]隐蔽监视 💂公开监视

[image]身体暴力（含酷刑） [image]警察巡逻 [image]道路封锁 [image]服务提供商协助调查

- 2个子项目 [image]移动网络运营商 [image]其他可能出卖您的服务商和机构

🎯有针对性的数字监控

- 5个子项目 身份验证绕过 [image]黄貂鱼 恶意软件 [image]网络取证 [image]恶意女仆和查抄

🚨

逮捕

🚨报警系统 [image]警犬 [image]警卫 🛖抄家 🕵身份检查 🚔增加警力 🌎跨国维稳 [image]警察巡逻 [image]道路封锁

名词解释

[image]

自卫措施

[image]

降低镇压风险、缓解镇压影响的可能措施

[image]匿名着装 [image]匿名手机 [image]匿名购买 [image]反监视 [image]反攻 [image]避免自证其罪 [image]背景调查 [image]生物特征隐藏 [image]监视器排查 周密的行动计划 [image]隐姓埋名 分身 [image]计算机和移动设备取证 [image]数字技术限制和最佳实践 [image]DNA最小化方案 加密 [image]假身份 [image]手套 [image]掩盖写作风格 [image]元数据擦除和避免 [image]信息最小化原则 [image]关系网络图谱 [image]户外无设备对话 [image]物理入侵检测 [image]突袭应对措施 [image]镇压应对措施 [image]被捕支援 [image]地形侦查 [image]藏匿点或安全屋 [image]监控侦测 [image]防篡改准备 [image]自行车接力
[image]

名词解释

[image]

带有攻击树的威胁库用例示范

[image]

威胁库中的信息量巨大，可能会令人眼花缭乱。那如何在您的实际生活中、在特定项目中、或在行动时运用威胁库呢？本教程旨在帮助您使用攻击树来浏览威胁库。

攻击树是一种工具，用于在特定情境下通过树形结构可视化展示对手可能成功攻击您的各种方式，从而促进头脑风暴。攻击树有助于通过建模对手可用的选项，理解计划或项目如何容易遭受镇压。

您可以自行进行这项威胁建模练习，但如果您计划与他人共同执行某项行动，那么建议您与队友们一起进行这个步骤。本练习对新手和有经验的团队都有益处。 即使每个人都已经拥有强大的安全实践，本练习也可以提供一种结构化的方法来确保不会忽视任何威胁，并帮助大家统一安全预期。

[image]

一个简单的例子：逃学一天

在考虑实际案例之前，我们先来看一个最简单的例子。假设你是一名学生，你和你的朋友想逃学一天，但不想让父母知道。在这里，你们的对手是整个学校系统。

立刻开始。

首先绘制根节点：它代表对手的目标。

在这个例子中，对手的目标应该是请家长 —— 让你的父母知道你逃学了。学校可能会打电话给你的父母或寄信给他们。或者你的其中一位老师可能会遇到你的父母并当面告状 —— 这可能发生在你的数学老师身上，因为他住在你家附近；或者，你的历史老师也有可能，因为他每个周末都和你的朋友的父母一起休闲。

你需要绘制出所有这些节点。

[image]

图中灰色的为根结点。

只要一个节点为真，那么该节点的后继节点中就必须有一个为真。

比如，“把你逃学的事情告诉你家长”这个节点为真，那么它的3个后继节点中就必须有一个为真。

对于 “你的一位老师碰巧遇到你父母就当面告你状了” 这一条件如果要成立，那么它下方的两个后继节点中就必须有一个为真。

换句话说，如果你能从最外层节点追踪到根节点，且沿途所有节点均为真，则意味着根节点为真，即攻击成功。

一个现实的例子：临冬城发生骚乱

假设你和一些同志正在准备在临冬城发动一场骚乱。你们想制造一些破坏，但又不希望被抓住…… 于是你们使用威胁库以提前规划防御。你们打印出威胁库的文档，带上笔和纸，与队友们在户外且不使用电子设备的情况下会面，以商讨防御措施。

讨论的目标：绘制出攻击树，识别适用于你们当前情境的技术和防御

措施，并决定如何实施这些措施。非常建议在行动结束后进行回顾复盘，以总结经验教训，下一次可以做得更好。

绘制攻击树

在此示例中，对手是临冬城政权及其镇压机器 - 警察，他们的目标是获取足够证据以证明你们参与了骚乱，以说服法官给你们定罪。你现在需要绘制攻击树，以展示这些镇压者实现该目标的途径。

注：对于复杂的行动，建议将其拆分为阶段/步骤（例如计划、准备、执行、解散），并为每个步骤绘制攻击树。

从根节点开始。

对手的目标是：定罪。所以根节点就是：

[image] 临冬城“骚乱”攻击树（根节点）。

接下来开始添加根节点旁边的直接子节点。换位思考，现在你扮演镇压当局。在这个阶段，你应该添加你能想到的任何内容，即使你不确定它是否适用于该项行动。换句话说，就是要假设镇压当局不惜余力地发疯。你可以向各个方向扩展树，使其更加紧凑。

[image] 临冬城“骚乱”攻击树（第一层节点）

您可以使用威胁库来构建攻击树 —— 阅读 相关镇压战术知识 可以帮助您更好地了解对手可用的所有攻击选项。

创建攻击树需要一定的思维模式，这需要练习。

当不再需要添加更多节点以完成攻击目的、并且您能想到的所有攻击方式都已经包含在内时，攻击树就完成了。

[image] 临冬城“骚乱”攻击树（完整版）。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

对于上述图像，请点击右上角三个点 “… - 查看原始内容”，以得到大图。

识别镇压战术

通过将攻击树中的节点与威胁库中的镇压战术进行匹配，以识别树中的每个节点所具体代表的威胁形式。攻击树可能很“大”，建议您逐个分支进行操作，以避免迷失方向：最好从靠近根节点的第一层后继节点开始，然后逐步向上推进。

[image] 临冬城“骚乱”攻击树（“突袭抄家”分支）

您可以从“通过对已知嫌疑人的住所进行突袭搜查以获取证据”分支开始：

- “通过对已知嫌疑人的住所进行突袭搜查以获取证据”与“抄家”匹配。
- “从扣押的电子设备中收集证据”对应的是“有针对性的数字监控：恶意女仆和查抄”—— 因为他们会物理访问您的电子设备；以及“有针对性的数字监控：身份验证绕过”—— 如果他们试图猜测您的密码或破解您的加密。
- 其他节点与任何内容均不匹配，它们只是房屋搜查的一部分。

直接点击内嵌链接进入具体页面即可。

在此阶段，评估所列出的镇压战术带来的风险可能有所帮助 —— 这将决定是否以及如何从根本上缓解每个风险。参见本页面下述“评估

风险”一节，了解如何使用“可能性”和“影响”概念评估镇压战术的风险。

然后继续处理下一分支，直至覆盖整个流程图，形成一张表格。

表格的开头看起来像这样：

[image]

鉴定自卫措施

接下来，通过查看威胁库针对表格中镇压战术所建议的自卫措施，来确定要实施哪些措施。

在上述示例分支中，您将决定实施以下措施：

- 对于“抄家”，实施“镇压应对措施”、“突袭应对措施”、和“藏匿点或安全屋”。您不希望实施“隐姓埋名”措施，因为您决定不走逃亡那条路。或者暂时没有那个必要。
- 对于两个“针对性数字监控”镇压手段，对应的应该是“数字技术限制和最佳实践”。

所以，接下来您将更新上述表格。

决定如何实施自卫措施

最后，您需要决定如何实施表格中的自卫措施。阅读威胁库中的相关条目可以提供一些思路。您对每种镇压战术的风险评估结果有助于您确定应投入多少精力到自卫措施中。

您决定采取以下实施措施：

- “镇压应对措施”：由于您和队友们都住在同一个地方，存在因突袭搜查而被集体逮捕的风险。所以您需要确保其他队友都知道如何在这种情况下为您提供支持。

- “突袭应对措施”：您决定不再把准备在行动中使用的条幅或者烟花等物品存放在床下。

- “藏匿点或安全屋”：您决定在附近森林中埋藏一个防水容器来存放烟花。当有人取用时，必须戴手套并确保周围无人。

- “数字技术限制和最佳实践”：你们的设备已经加密，而且你们本来就不用电子设备来讨论行动相关的问题。你们必须确认手机在开机并锁屏状态下加密功能是否有效，如果不确定的话。

在这个阶段，重新评估这些镇压战术的风险是有用的，以确保你们决定实施的应对措施已经足够可以降低风险。

接下来进一步更新上述表格。

[image]

彻底销毁您的笔记，或者...

本练习中记录的笔记不应保留，因为它们可能被视为串谋的证据。

对此您有两种选择：

1、练习结束后，请将笔记完整背诵下来，然后将其烧毁 —— 放心很容易记住的，因为这是您主动思考的结论。要注意的是，如果想要在未来重新查看并扩展这些笔记，届时就只能凭记忆重建它们了。

2、或者，在练习结束时，使用**Tails**将笔记手动复制到加密的**USB**设备中进行数字化（记得遵循“数字最佳实践”）。您可以使用

LibreOffice Draw（Tails默认包含）来绘制攻击树。一旦笔记被数字化，不应将其打印出来，因为打印机会留下痕迹，但可以手动将其再次抄写到纸上，以便在没有计算机的情况下查看。用过的纸张遵循阅后即焚。

进行行动回顾

行动结束后，您和同伴们需要花些时间以进行行动回顾：在户外且不使用电子设备的对话中，讨论哪些方面做得很好、哪些方面存在问题，以及攻击树的覆盖范围、或自卫措施的实施方式等，是否还有改进的空间。该流程的具体步骤见：[image]场内协作和场外接应同样重要：整体安全S01E12 - 紧急撤离和汇报评估

风险评估

“风险”是技术影响程度与发生可能性的综合衡量指标。

如果某项技术的影响程度很高，但发生的可能性极低，则可能被视为低风险。相反，如果某项技术的影响程度中等，但发生的可能性较高，则可能被视为高风险。如果认为某项技术的风险较高，则应更彻底地针对其制定应对措施。

比如，对于俄罗斯无政府主义者纵火焚烧征兵办公室的行动，法医取证的DNA技术就属于高风险。因为它具有高影响（与火灾现场的DNA匹配是法庭上的有力证据）和高可能性（在大多数情况下，DNA取证技术在纵火调查中被系统性地使用）。

影响

“影响”是衡量镇压手段被使用的后果的指标。它取决于镇压战术的类

型：

- 威慑战术：其“影响”取决于目标是否被成功威胁到（从精神层面上被控制住）。

- 指控战术：其“影响”取决于收集到的证据的“可靠性”（能说服法官和陪审团的都是“可靠”）。

- 逮捕战术：其“影响”取决于目标是否被成功逮捕。

可能性

“可能性”是衡量对手采用某种镇压战术的可能程度的指标。

对手的资源投入水平与风险增加之间的关系

如果对手已经投入较多资源以压制某项行动，那么某种相关的镇压战术就更有可能被使用，从而增加其“可能性”；并且会被更彻底地使用，从而增加其潜在“影响”。总体而言，如果对手感到某项行动对其构成了更大威胁，就会投入更多资源来压制该行动。

例如：

- 在大多数情况下，DNA法医鉴定会被系统性地用于纵火案调查。如果对手资源有限，搜查可能仅限于门把手等明显表面。如果对手拥有更多资源（例如纵火造成了大量破坏），现场更可能被彻底搜查以寻找DNA证据。

- 在大多数情况下，如果对手是国家，被归类为“恐怖主义”的案件、或者对于被描述为“对国家安全构成威胁”的行动的侦查，将获得大量的资源支持。国家可能会投入大量资源调查起义期间发生的行动，因为起义被视为对国家完整性的威胁。

缓解措施可降低风险

通过采取适当的缓解措施，您可以降低对某种镇压战术的脆弱性，从而减少其潜在的“影响”。

例如，您对DNA鉴定技术存在脆弱性，因为人体会不断脱落DNA；如果在点火时应用“DNA最小化方案”，您对DNA鉴定技术的脆弱性将降低。

风险与本地环境

建议您平日多了解对手在压制某一类行动时的习惯手段和动机（即对局势分析的战术性使用），可以帮助您推断对手可能使用的手段的范围，以及他们使用这些手段的彻底程度。旁观发生在其他地区的镇压行动，也可以帮助您理解某一镇压手段在特定环境中的使用方式。相关内容在IYP的列表-5“维稳面面观”中收纳。

最后

威胁库始终欢迎外部贡献，例如：

- 对现有镇压手段、自卫措施、或压制性操作的更改意见。
- 对新的镇压手段、自卫措施、或压制性操作的添加提议。
- 不同类型项目的攻击树。
- 将威胁库翻译成其他语种的合作关系；包括进一步本地化的工作。

[image]

抄家

抄家是指对手对住宅进行突击搜查，以扣押物品、逮捕住户、或强行安装监控设备。

通常什么时候发生

抄家经常发生在：

- 通常在清晨，天亮之前，屋内的人正在熟睡，最猝不及防的时候。

- 在某些情况下，抄家会在白天进行。例如，当突袭的目的之一是查获正在运行的数字设备的时候 —— 此时其加密功能可能无效。这种情况下对手可能选择在白天进行突袭，因为数字设备在用户清醒的情况下更可能处于运行状态。

抄家的目的

对手实施抄家的目的可能包括：

- 扣押物品以寻找证据或进行网络映射（连锅端）。常见的扣押物品包括电子设备、文献、可用于行动的材料以及衣物。在某些情况下，对手会扣押昂贵物品（如电脑、打印设备），以破坏目标组织的运作能力。

- 逮捕住宅内的居民。
- 在住宅内安装监控设备。

其他考虑因素

在某些国家，当国家机器进行突袭时，仅允许搜查搜查令中列名的房间。如果您和您的组织有面临此类风险的可能性，请参考本地法律，记住您的权利。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]
[image]

警犬

警犬是经过训练以被用于检测气味的犬类。可用于检测爆炸物或毒品等物质、追踪目标人员，以及参与气味辨认程序以确定目标人的气味是否存在于某些物体上。

□

延伸：据报道，中国西南部云南省的科学家克隆了警犬，他们称之为“警犬中的福尔摩斯”，希望此举能帮助减少警犬的训练时间和成本。https://www.theguardian.com/world/2019/mar/20/china-clones-sherlock-holmes-police-dog-to-cut-training-times-report

气味是由物质释放的挥发性化合物引起的。例如，旧书的气味是由纸页不断分解时释放到空气中的化学化合物引起的。

人体气味，即所谓的体味，是由水分泌物（汗液）、油分泌物（皮脂）、皮肤碎屑和身体开口（如口腔、鼻腔等）释放的化合物引起的。每个人都有相对独特且随时间相对稳定的标志性气味。

犬类的嗅觉比人类的嗅觉复杂且发达得多。犬类可以：

- 检测非常微弱的气味。
- 在混合气味中识别单一气味。
- 判断气味来源的方向。

- 以极高精度感知气味强度。例如，若两种气味在相似条件下存在，它们可判断哪一种气味更强烈，从而推断其更近期。

检测物质

对手可以训练警犬来检测爆炸物、毒品、助燃剂、或较少见的电子设备等物质发出的气味。

对手可以使用警犬：

- 在行动现场或房屋搜查、秘密入户搜查时，确定某种物质是否存在，并定位其位置。

- 在身份检查时，确定被检查人员是否携带或接触过某种物质。

在许多国家，国家机构会使用警犬在边境、机场、火车站等场所检测“非法物质”。

追踪人员

当人步行移动时，会留下由以下成分组成的气味轨迹：

- 其自身体味，包括脚部分泌的水分（汗液）和油脂（皮脂）气味，以及身体脱落的皮肤碎屑气味。汗液和皮脂气味会渗透鞋子，包括橡胶鞋。

- 附着于脚底或鞋底的物体气味。

- 如果穿着衣服：衣服上脱落的颗粒的气味。

- 如果穿着鞋子：鞋子材料的气味（橡胶、皮革等）。

- 如果踩踏过活的植物，包括草：被踩到的植物释放的汁液气味以及破碎部位细菌分解的气味。

- 如果踩到的是小昆虫或其他小型动物，会带有动物尸体的气味。

对手可以训练警犬追踪此类气味的轨迹。

追踪方法有两种：

- 第一种方法：向犬只提供气味样本（例如嫌疑人穿过的衣物、摸过的东西），并要求其定位并追踪含有该气味的轨迹。此方法更可靠。

- 第二种方法：不向犬只提供气味样本，直接要求其定位并追踪轨迹。此方法可靠性较低。

在许多国家，国家机构使用嗅探犬追踪嫌疑人，但由于犬只被认为不可靠，追踪结果在法庭上不被视为有力证据。在某些国家，上述第一种方法的追踪结果被视为有力证据，而第二种方法的追踪结果则不被视为有力证据。

侦查犬通常可在气味痕迹留下后两至三天内跟随，甚至在某些情况下，根据不同因素，可长达两至三个月。

影响侦查犬在气味痕迹留下后较长时间内跟随能力的主要因素包括：

- 犬只及其训导员的训练水平。

- 人类在气味痕迹上或附近的活动（比如游泳过河、用很强烈的异味掩盖等等）。

- 风力。空气流动可能分散构成气味痕迹的挥发性化学物质。
- 降水。雨水、雪或露水可能溶解构成气味轨迹的部分挥发性化学物质。

气味排列测试

对手可训练警犬参与气味排列测试。

设置气味排列测试时，对手会从嫌疑人及另外5至10人处采集气味样本，并将样本并排放置于空旷房间内，确保样本间保持一定距离。随后，向犬只提供一种目标气味，并要求犬只判断是否有任何气味样本与该气味匹配。

通常，犬只被提供在行动现场收集的疑似携带嫌疑人气味的物品：若犬只判断嫌疑人的气味样本与该物品的气味匹配，对手可推断嫌疑人曾接触该物品并可能参与了该行动。

气味辨认程序的结果通常不被视为法庭上的有力证据。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]

关系网络图谱

网络关系图谱练习通过创建关系图谱来呈现您与关系网络中不同人员之间的关系亲疏及性质。以便批判性地审视这些联系。

此项练习旨在提升您对交往对象做出明智且批判性筛选的能力，最终目标是增强您的关系网络抵御 渗透者 攻击的能力。

[image]

返回 ：[image]S01E03-T1 周围是谁？可视化人际关系图谱

此项练习的核心理念是帮助您不仅在亲密团队层面思考，更要从全局视角进行思考，包括您不太熟悉的人，甚至可能包括您根本不认识的人。

练习的方法是问自己一系列结构化的问题，这些问题揭示了您与人际网络中所有人之间的安全级别，然后，您根据这些关系绘制一张图，区分您信任的人和您想要深入了解的人。

这项练习适合在相对平静的时候进行。

请注意：这样的关系图谱对您的对手来说非常宝贵！所以您在使用完之后应该彻底销毁它！

[image]

返回 ：[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

返回：[image]如何组织社交空间

[image]

在本站专题栏目中了解更多保护措施 🎀人际安全&关系结构革命-RelationshipsRevolution

此自卫措施用于应对的镇压手段

[image]

避免自证其罪

避免自证其罪意味着不向对手提供可能被用来指控您或您的同志的信息。大量定罪都是基于通过自证其罪获得的信息。

[image]

返回：[image]您是如何被困住的：审讯心理学 S07E01

返回：[image]巧妙的威胁：审讯心理学 S07E02

不要跟警察说话

如果您被国家对手逮捕，尽可能不要跟警方交谈。任何沟通都可能被用来指控您或您的队友。

此规则的例外情况包括：

- 在许多情况下，您可能会被迫向警方提供某种形式的身份证明（通常是您的姓名、出生日期和地点），以避免被捕或其他负面后果。
- 在某些情况下，您可能被迫向警方提供您的生物特征信息（🎭面部识别、[image]指纹、DNA

推荐专业的审讯心理学知识（邀请中文译者）：

https://www.notrace.how/resources/download/comment-la-police-interroge-et-comment-sen-defendre/how-to-defend-yourself-during-a-police-interrogation.pdf
[image]

返回：[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

信息最小化原则

采取 [image]信息最小化原则 ，简单说就是，没有直接参与某事的所有人都不应该知道此事。不管某人与您多亲密、多值得信任，那都是另一回事，只要他/她没有直接参与，就不应该了解。

激进派人士最大的心魔是孤独，不被理解不被“看见”是一种真正的折磨，这种折磨让他们很容易下意识向朋友、战友或狱友吹嘘自己的所作所为。这是非常危险的。非常容易被您的对手得知。一定要管住自己。

数字最佳实践

遵循 [image]数字技术限制和最佳实践 。特别是：

- 不要让任何可能将您定罪的信息（短信、照片等等）通过您的手机，即使您使用端到端加密的消息应用程序，也不要。短暂保存也不要。 [image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

- 尽可能不使用社交媒体，或者至少千万不要在社交媒体上发布任何有可能证明您参与了某项行动的信息。社交媒体是国家暴力机器的宝库。 [image]社交媒体上的行动主义安全性:框架手册

- 在起义行动期间不要拍照录像。尤其是未经同意的对着行动者的脸部拍摄，应被视为告密行为。这点要纳入安全原则中。
  BACK [image]“不要再拍了！请关闭设备删除影像”

此自卫措施用于应对的镇压手段

[image]
👁️□🗨️□

大规模数字监控

对全部或大部分人口的数字通信进行大规模收集、存储和分析。所有国家都喜欢做这事，区别只限于其具体能力决定了其能做到什么程度。

棱镜是在此规模最大的、最系统的案例。中国的天网工程也是。俄罗斯的SORM也是。

□

延伸：https://web.archive.org/web/20250523052240/https://iyouport.substack.com/p/lr--6f2

延伸：https://web.archive.org/web/20250523054741/https://iyouport.substack.com/p/7a9

延伸：https://web.archive.org/web/20250305214504/https://iyouport.substack.com/p/4d2

https://iyouport.substack.com/p/lr--6f2?utm_source=publication-search

大规模数字监控依赖于从多种来源收集数据：金融交易、边境管控、智能手机的GPS定位，甚至"智能"路灯和广告牌。所谓的"智能"越多，数字面包屑就越多。

□

延伸：https://web.archive.org/web/20250202150421/https://iyouport.substack.com/p/075

存储容量的技术进步使得大量数据能够存储在国家控制的数据存储设施中。处理能力的技术进步导致对这些数据的自动化分析已成为可能，从而促进了全球执法和情报机构的工作。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

📌 对应的镇压战术：威慑、指控。

自卫措施

[image]

偷拍

隐藏监视摄像头是很容易的事。

延伸：https://iyouport.substack.com/p/46b

对手可以在任何能看到目标人或目标监控区域的地方隐藏视频监视设备。

值得注意的地点包括：

- 目标人住所的客厅。
- 靠近目标住所的建筑物的窗户，能看到住所的入口，和/或主要房间窗户。
- 靠近藏匿点或安全屋，如意大利发生的情况，警方安装了运动感应激活摄像头以监控一个森林中的藏匿点。

捕获的图像可作为法庭证据。无关犯罪证据的日常图像也能揭示目标人的许多信息，并有助于创建社交网络映射，以实现连锅端。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
□

身份验证绕过

身份验证绕过是指攻击者绕过保护数字设备访问权限的全盘加密机制的过程。攻击者可以通过人为错误、弱密码或技术漏洞来实现身份验证绕过。

攻击者可以通过以下方式实现身份验证绕过：

- 在设备开机状态下访问设备（因此其加密功能无效）。
- 找到写在某处的密码。
- 通过审讯心理操纵（包括某些情况下使用身体暴力）迫使设备所有者交出密码。
- 视觉拦截：通过隐藏的监视摄像头或内部线人观察设备所有者输入密码。
- 暴力破解：通过反复自动认尝试猜测加密密码。
- 通过远程安装的恶意软件或物理访问手段入侵设备。
- 利用加密过程实现层面的漏洞。

□

延伸：https://start.me/w/8LRjvQ

延伸：https://start.me/w/OaLzjO

📌 对应的镇压战术：指控。

□

延伸：https://iyouport.substack.com/p/e3b?utm_source=publication-search

延伸：https://iyouport.substack.com/p/-cia-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/d09?utm_source=publication-search

延伸：https://iyouport.substack.com/p/c53?utm_source=publication-search

自卫措施

[image]

返回：[image]在坏人强行访问您的设备的情况下抹除数据

返回：[image]如果您的手机被盗或被警察抢走...

返回：[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？

返回：[image]如何保持 Android 设备免受警察的侵害

镇压行动案例

[image]
[image]

数字取证

数字取证是指检索、存储和分析可用于调查的电子数据。这包括来自计算机、手机、硬盘和其他数据存储设备的信息。

例如，数字取证可以用于从计算机硬盘中恢复一个“已删除”的文件、恢复“已删除的”手机网页浏览历史、或者确定服务器是如何被黑客入侵的，等等。

[image] 2013年，以色列手机黑客公司Cellebrite通用取证提取设备 (UFED) 从 iPhone 4S 中提取数据。
□

延伸：https://iyouport.substack.com/p/c94?utm_source=publication-search

延伸：https://iyouport.substack.com/p/--f02?utm_source=publication-search

[image]

返回：[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

返回：[image]让政府机构从您使用的应用程序中提取大量数据的秘密技术：云取证

[image]

返回：[image]做移动设备取证和数字调查的开源平台

📌 对应的镇压战术：指控。

【2026/04/10 更新】

【新闻】FBI已成功通过通知存储功能从目标人的iPhone中提取了“已删除的”**Signal**消息。通知存储是系统存储所有通知的地方，这些通知最多可保留一个月。

通知存储会保存所有即时通讯应用的数据，对于加密IMs来说这是一个漏洞。但您可以关闭它。

[image]

前往 iOS 设置 → 通知 → [应用名] → 显示预览，并将选项设为“永不”。

您也可以直接通过“设置 → 通知 → 显示预览 → 永不”进行全局设置。

此外，如果您真的想完全掌控自己的数据，别忘了在 iCloud 设置中开启“高级数据保护”功能。

为确保万无一失，还建议在 Signal 中禁用该功能。在 Signal → 设置 → 通知 → 将“通知内容”设为“没有名字或内容”。

自卫措施

镇压行动案例

[image]
🕷

人肉搜索

人肉即doxxing，是指未经目标对象同意而公开其私密信息，以伤害目标对象、或怂恿他人伤害目标对象的行为。非国家对手最常使用这种手段。

[image]

返回：[image]给活动家的反人肉指南

📌 对应的镇压战术：威胁

自卫措施

[image]
🌎

跨国维稳

跨国维稳（准确说是国际合作）指的是不同国家执法和情报机构之间的信息交换/共享。

延伸：https://iyouport.substack.com/p/c20?utm_source=publication-search

延伸：https://iyouport.substack.com/p/protonmail-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/82d?utm_source=publication-search

延伸：https://iyouport.substack.com/p/8f5?utm_source=publication-search

延伸：https://iyouport.substack.com/p/-192-?utm_source=publication-search

国际合作可用于：

- 情报交流。
- 协助跨国界对嫌疑人进行指控、逮捕和驱逐。

- 国际合作可通过非正式渠道进行，也可通过正式组织如国际刑警组织来实施。（附 国际刑警组织通缉人员数据库 ）

📌 对应的镇压战术：逮捕、指控。

镇压行动案例

[image]

突袭应对措施

只要镇压者认为“足够必要”这样做，且他们得知了您的住处，他们不仅有可能偷偷闯进来，还可能直接破门而入。“突袭应对措施”就是指您需要对这类状况有所准备。

一项重要的预防措施是 —— 尽量减少那些您不想让对手在突袭中发现的东西。特别是：

- 对所有数字设备进行加密 ，并在睡觉前或外出时关机，以使加密生效。
- 激进行动中使用的物品事实上大部分都是“合理合法的”，比如[image]手套 、漂白剂、汽油等等。它们单独放置时合法，但如果您把它们打包放在一起，就很容易被镇压者解读为“犯罪现场搜出作案证据”。请把手套放在洗碗台旁，把漂白剂放在洗衣机旁，把汽油放在车库里。
- 如果您的确制作了燃烧瓶还没来得及使用，或者类似的材料，就不应该放在家里了，请把它们存放在[image]藏匿点或安全屋中，或者最坏的情况是，让它们在您家短暂地流通一段时间，切勿长期保存！以及，在大多数情况下，我们同时认为您也不该在家中存放无政府主义文献，尤其是直接行动相关的技术文献。 再次声明：请使用**Tor**网络浏览本站。

此外，为检测对手是否在突袭您家期间触碰过您的任何电子设备，请使用[image]防篡改准备 。

此自卫措施用于应对的镇压手段

[image]

开源情报

开源情报 (OSINT) 是指从公开来源（社交媒体、新闻媒体、博客、论坛、公共记录等）收集和分析数据。

[image]

返回：[image]攻击者如何收集有关目标的情报？他们能了解你多少？

返回：[image]为什么说您值得了解一些数字开源情报收集和调查的方法：对抗性思考方式

返回：[image]如何跨社交媒体平台追踪目标人：对抗性思考方式

返回：[image]间谍机构使用的开源情报监视方法

返回：

延伸：如果您想要更多学习相关技术，可参考我们的主题列表（随时间推移工具类条目可能过期。请着眼于思考方式的练习）：

- https://start.me/w/L9jode
- https://start.me/w/YBqAGq

- https://start.me/w/lb12DK

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
👁️‍🗨️

大规模数字监控

对全部或大部分人口的数字通信进行大规模收集、存储和分析。棱镜是在此规模最大的、最系统的案例。中国的天网工程也是。

延伸：https://web.archive.org/web/20250523052240/https://iyouport.substack.com/p/lr--6f2

延伸：https://web.archive.org/web/20250523054741/https://iyouport.substack.com/p/7a9

延伸：

[image]
泄露：中国庞大的警察数据库
【2021年5月13日存档】数百万泄漏的警察档案详细记录了对中国维吾尔族人口的监视
[image]https://web.archive.org/web/20250305214504/https://iyouport.substack.com/p/4d2
https://iyouport.substack.com/p/lr--6f2?utm_source=publication-search

大规模数字监控依赖于从多种来源收集数据：金融交易、边境管控、智能手机的GPS定位，甚至“智能”路灯和广告牌。所谓的“智能”越多，数字面包屑就越多。

延伸：https://web.archive.org/web/20250202150421/https://iyouport.substack.com/p/075

存储容量的技术进步使得大量数据能够存储在国家控制的数据存储设施中。处理能力的技术进步导致对这些数据的自动化分析已成为可能，从而促进了全球执法和情报机构的工作。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

📌 对应的镇压战术：威慑、指控。

自卫措施

[image]

防篡改准备

[image]

上图就是一个非常简易的防篡改方法 —— 一盘黄豆和黑豆的混合，两种颜色混合出了独特的复杂图案。现在把您的敏感电子设备塞进豆子里，然后用相机拍下呈现的图案。如果等您回家时发现豆子的图案发生了变化，则说明电子设备被人动过了。

防篡改准备是指采取预防措施，以便在某些特定物品遭到攻击者物理接触时能够检测到的过程。

防篡改准备可用于：

- 监测是否有攻击者偷偷潜入您的房间并在您的电子设备上安装了恶意软件。
- 监测对手是否已经发现了您的[image]藏匿点或安全屋

[image] 把指甲油涂在螺丝上

防篡改准备的示例包括：

- 将指甲油涂在笔记本电脑的螺丝上并拍照保存。由于指甲油的图案复杂（类似火漆封印），对手很难在不改变图案的情况下卸下螺丝。当您想要验证笔记本电脑是否被拆卸过时，可以重新拍摄螺丝照片，并将其与原始照片进行比较：如果指甲油的图案相同，则表示电脑没有被拆开过。
- 把电子设备塞进一个透明的盒子里，盒子里装满不同颜色的小

石子（例如，一半黑色鹅卵石，一半白色鹅卵石），并拍摄盒子侧面的照片。由于这种混合物的图案复杂，对手很难在不改变图案的情况下取出电子设备。因此，当您返回家中时，可以重新拍摄盒子侧面的照片，并将其与原始照片进行比较：如果混合物图案相同，则表示电子设备未被访问过。要确保您无法随身携带的所有重要电子设备始侵入在这样的盒子里。

[image]

返回-监测物理入侵的小工具：[image]物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪

防篡改软件和固件

防篡改固件与[image]数字技术限制和最佳实践 方案兼容：笔记本电脑可选用 Qubes OS 或 Tails，智能手机可选用 GrapheneOS。

对于 GrapheneOS，Auditor 应用可让您在固件或操作系统软件遭到篡改时收到通知 —— 它会发送电子邮件给您。

对于 Tails 或 Qubes OS，Heads 能在您输入启动密码前执行相同检测（在受支持的设备上）。但 Heads 安装过程较为复杂，用起来则很简单。外出时请随身携带 Heads USB 安全密钥，并在可信赖的朋友家中预留备份，以防密钥意外浸水损坏。更多信息请参阅《Tails 最佳实践指南》。

若 **Auditor** 或 **Heads** 检测到了某设备遭篡改，请立即将其视为不可信设备。[image]计算机和移动设备取证 分析可揭示入侵途径，有助于防范再次发生。您可联系 Access Now 数字安全热线等服务机构，但建议勿向其发送任何个人数据。

此自卫措施用于应对的镇压手段

[image]

藏匿点或安全屋

推荐印尼无政府主义创办的“安全屋网络”项目，对于面对黑头套/强迫失踪威胁的人们来说，可靠的藏身之地至关重要。在这里看到详情：https://www.firefund.net/indonesiansafehousenetwork

藏匿点和安全屋是用来逃亡过程中藏身、或者存放敏感材料的两种方式。

敏感材料不要存放在家中，即便您被抄家 或遭到[image]隐蔽性地突袭住所 ，对手也无法找到它们。

藏匿点是一个隐蔽的地方，通常位于户外，不太可能被人发现。安全屋是指对手不知道您正在使用的房屋、公寓或其他空间。 并且他们很难查到。

藏匿点和安全屋各有优势：

- 设置储藏点更加容易。
- 更容易实现[image]DNA最小化方案 。
- 更改藏匿点的位置更容易。狡兔三窟。
- 安全屋提供了更多的存储空间，同时可用于藏身避险。

可作为藏匿点的示例包括（并不限于）：

- 远离小路的树林里某个特定位置埋藏的铁盒子（降低被徒步者发现的可能性）。
- 某个废弃建筑物中的小角落。

安全屋的可能示例包括（并不限于）：

- 匿名租用的房屋、公寓或其他空间 —— 使用[image]假身份 和现金 。
- 您信任的人的住所，此人愿意承担这种风险，并且尤其是，此人距离您的敏感行动关系网络足够远，以至于可能没人会把此人与您的正义事业联系起来。

如果对手发现了藏匿点或安全屋，他们就可以开始监视它，以便在您进入时识别您，就像在意大利发生的情况那样，镇压者安装了运动激活监视器来监视森林中的藏匿点。

因此，当进入藏匿点或安全屋时，您可以：

- 实行[image]反监视 以甩掉[image]物理监控（上岗）
- [image]匿名着装 以应对被检查和记录的风险。
- 进行[image]防篡改准备 以确保藏匿处或安全屋不会被对手进入。

推荐资料《Security Culture and Safe Houses》以了解无政府主义者使用安全屋的历史视角。

[image]

注：中文文档为AI翻译的结果。我们还没有时间进行具体校对。诚邀有能力的朋友进行详细编译。如果您有意，欢迎联系我们。

安全文化和安全屋.pdf

此自卫措施用于应对的镇压手段

[image]
[image]

其他可能出卖您的服务商和机构

除移动网络运营商外的其他服务提供商也都可能向您的对手提供有关您的私密信息。

商店

实体商店和数字商店都可以提供您的购买信息，包括：

- 以姓名为线索：该姓名对应的购买商品及购买日期。
- 以商品或商品类别为线索：购买该商品的人的姓名及购买日期。

此外，实体商店还可提供：

- 商店监控摄像头拍摄的监控录像。
- 商店员工的证词（见“平民告密”页面），例如关于某次特定购买行为的购买者外貌特征。

银行

银行可以提供：

- 您的银行账户交易记录，包括使用银行卡进行的任何购买或取款的日期、地点及金额。

- 自动柜员机（ATM）监控摄像头拍摄的监控录像。

互联网服务提供商

互联网服务提供商可以提供：

- 如果您遵循数字最佳实践并使用Tor：他们可以提供关于您互联网活动的元数据，例如您使用互联网的时间。

- 如果您没有使用Tor：他们可以提供您的几乎所有互联网活动，包括您访问的所有网站列表。

延伸：https://iyouport.substack.com/p/9db?utm_source=publication-search

延伸：https://iyouport.substack.com/p/facebook-1-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/facebook-2-?utm_source=publication-search

在线服务

网站、电子邮件提供商和其他在线服务可以提供：

- 您通过该服务进行的所有未加密通信的内容（例如社交媒体帖

子、未加密的电子邮件等等）。

- 您通过该服务进行的加密通信的元数据（例如加密电子邮件的发送者、接收者和日期）。

邮政服务

邮政服务可能允许对手监控您的邮件和包裹。

国家机构

国家机构可以提供他们掌握的关于您的任何信息，包括您的地址、税务记录、健康信息等等。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

审讯心理学

审讯技巧（审讯心理学）是指对手在审讯过程中用于从被捕者口中获取信息的手段。

[image]

返回本站《 心理安全 》专题栏目，获取更多审讯心理学相关知识。

审讯技巧可能包括说谎、威胁、制造内疚、羞耻或自豪感，试图表现得友好和乐于助人，或者相反，表现得威胁和暴力等。在某些情况下，可能包括身体暴力，即酷刑和强奸。

推荐书目

参见《警方如何进行审讯以及如何应对》，以获得警方审讯技巧的全面概述。

对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

身份检查

身份核查是指国家通过要求个人提供个人信息、出示政府颁发的身份证件，或采集其生物识别信息（如面部照片、指纹、DNA）并与数据库进行比对，以验证个人身份的过程。身份核查可能成为盘问和施压的借口，并可能导致对个人随身物品的强行搜查。

配合身份核查会使国家获取您的个人信息，这有助于他们绘制您的社交网络，若你被通缉，还可能导致您更容易被逮捕。

无法配合或拒绝配合身份核查的后果高度依赖具体情境，但可能包括被强制采集生物特征信息（或在不知情的情况下被采集）、被拘留，以及被驱逐出境。

被身份检查针对的可能性取决于具体情况、以及您在国家机器眼中的形象。如果您从事不引人注目的活动、并且穿得看起来像个有钱人，被针对的可能性就较低。如果您被视为潜在犯罪分子或“非法移民”，或者在进入或离开起义现场时，被针对的可能性就会较高。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]
[image]

指纹

指纹取证是对指纹的收集、存储和分析的过程。

采集

指纹是手指上的水分和油脂留在您触摸的表面上的印记，可以从这些表面上采集。也可以直接从手指上采集，使用墨水或其他物质（首先将手指浸入墨水中，然后放在纸上，在纸上留下印记），或者使用电子指纹扫描仪。

分析

由于指纹几乎是唯一的且在个人一生中基本保持稳定，于是可以通过比较两枚指纹来确定它们是否属于同一个人。

留在物体表面的指纹会随着时间的推移和在某些条件下（例如与丙酮接触）而退化，并且必须包含足够的细节才能在比较中发挥作用（回忆您在新手机上录入指纹的过程）。

此外要注意的是，在某些表面，如金属表面，指纹油脂与金属的反应有可能在表面本身蚀刻出纹路，即使表面被丙酮浸湿的布擦拭后，指纹仍可识别。

指纹数据库

许多国家都拥有包含大量个人指纹的数据库，这些指纹通常在逮捕或刑事定罪过程中获取。

其他类型的印记

人类的手掌和脚趾可留下与指纹类似的印记，这些印记可采用相同方式采集和分析。在某些情况下，手掌印记会被定期采集并添加至指纹数据库。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

分身

分身是一种安全原则，即：将用于不同项目/任务的角色区分开运行，彼此间不产生任何关系。项目完成，相应的身份销毁。这样一来，不仅不容易被追踪到真实身份，并且便于控制 —— 遭受攻击和泄漏威胁的身份可以被清除掉。

我们曾经多次介绍过相关方法和思考方式。但都是数字形式的分身。现在需要您了解，它也可以适用于非数字形式，原理一样，只要您能把握住。

[image]

返回 - 演示：[image]大清洗 - 扫荡危险区域：完美隐身 S04E07

返回 - 演示：[image]在雷达下低飞：变得难以被追踪的简单方法 S03E07

具体方法：

[image]
[image]
返回：[image]袜子木偶 - 分身创建的小技巧
[image]
返回：[image]简易分身术：妥善管理您的在线身份并获得安全的方法

简单说 ……

数字分身的例子包括：

- 每个分身单独一套人设和全套联系方式。彼此间不产生任何关系。

- 每个身份使用一个Tails U盘 或Qubes OS。即便攻击者入侵了其中一个，也不会感染其他身份。

制作数字分身的思路简述

[image] [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] [image] [image] [image] [image]

非数字分身的例子包括：

- 在不同的场合使用不同的名字，例如与家人使用您的普通姓名，与朋友之间使用别名。别名可以特定于您与之互动的地点、时间或人群。这样，即使对手泄露了您的一个名字，也不一定会导致其他名字被泄露。 尤其是如果您有喜欢添加手机通讯录的朋友，这样做很有必要。 BACK 工具：[image]假联系人 - 保护手机通讯录

- 遵循 [image]信息最小化原则 ，仅在必要时且在必要的范围内共享敏感信息。

非数字分身的操作模拟：

[image]

返回：[image]技术增值部分-最简单的分身方法：完美隐身 S04E04

返回：[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方

法 S03E09

分身是一种非常有用的策略，还可以帮助记忆，尤其是当您同时处于多个项目运行状态中时，根据不同的人设姓名，您可以轻松记住哪个角色下必须执行 [image]反监视 、哪个项目中必须注意 [image]DNA 最小化方案 …… 等等。

采取此策略之前请进行威胁模型分析。

[image]

例如这样：[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

[image] 关于在线分身的框架。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] [image] [image]

此自卫措施用于应对的镇压手段

[image]

返回 - 工具：[image]虚拟手机号和马甲邮箱隐藏真实信息

[image]

隐姓埋名

“隐姓埋名”就是逃亡，脱离既定身份并以[image]假身份 开始新生活的过程。

这是一个高度复杂的状况，会很艰苦，非不得已不必如此。

[image]

返回：S04教程是关于逃亡过程中的安全技巧。从这里进入[image]S04完美隐身-总章节：机智是重要实力

有两种情况属于不得不采取隐姓埋名策略：

- 您确信已经被盯住了，每一刻都有可能入狱；或者您刚刚越狱。
- 您参加了秘密组织，即决定所有成员都应转入秘密状态的组织。

推荐以下文档资料

- Incognito - Experiences that defy identification

此自卫措施用于应对的镇压手段

[image]

物理入侵检测

针对一个空间（房屋或车辆内部）进行物理入侵检测，以检查可能的[image]隐蔽性地突袭住所 事件。

您可以通过确保某个空间内始终有人能够察觉到攻击者的入侵行为，或者使用视频监控系统监控该空间，来实现防范。 以下是一些相关软件，您可以是试试。

[image]

返回-工具：[image]物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪

返回-工具：[image]隐匿点/安全屋周围Wi-Fi入侵检测系统

如果您准备使用摄像机来监测一个空间的安全状况，需要知道：

- 该摄像机应该可以通过运动激活，如果被发现和被篡改，就会向您发送警报。
- 该摄像机可以放置在空间入口处和/或不显眼的位置。
- 仅在离开空间之前将其打开，并在返回后立即将其关闭，以避免它监视您。

此自卫措施用于应对的镇压手段

[image]
[image]

警方档案(网格)

警方档案是由执法机构保存的纸质或数字记录。警方档案包含涉及方方面面的海量数据，可以无限期或长期保存，并且可以使用数字工具进行高效的分析和交叉引用。

警方档案的典型例子包括：

- 政府颁发的身份证件数据库（身份证、驾驶执照、护照、社保卡等等）。
- 生物识别信息数据库（面部照片、指纹、DNA、步态等等）。
- 身份核查记录、罚款记录、逮捕记录、调查程序记录、司法程序记录、及定罪记录。

延伸：https://web.archive.org/web/20210716043727/https://iyouport.substack.com/p/06d

延伸：https://web.archive.org/web/20250306142821/https://iyouport.substack.com/p/faa

延伸：https://web.archive.org/web/20250202144356/https://iyouport.substack.com/p/f83

延伸：

[image]
泄露：中国庞大的警察数据库
【2021年5月13日存档】数百万泄漏的警察档案详细记录了对中国维吾尔族人口的监视
[image]https://web.archive.org/web/20250305214504/https://iyouport.substack.com/p/4d2
https://iyouport.substack.com/p/06d

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]
[image]

隐蔽监视

隐蔽的物理监视是指在监视人员不希望被监视对象发现的情况下，对人或活动进行直接的观察。

移动

移动物理监视行动通常由5至20名监视人员组成的团队使用多辆车辆进行，通常从静态阶段开始：在监视对象可能所在的地点（如其住所或工作场所）进行蹲点。当目标离开监视地点时，监视团队开始跟随目标，监视行动转入移动阶段。监视行动随后在静态阶段（目标停止时）和移动阶段（目标再次移动时）之间交替进行。

移动物理监视的示例包括：

- 根据目标的出行方式选择适当的监视行动方式。例如，若目标乘坐车辆，监视团队必须使用车辆；若目标步行，监视团队可能更倾向于使用步行跟踪。

- 利用掩护和隐蔽措施避免被目标发现。例如，监视车辆可藏身于其他车辆之后，步行监视人员可融入人流之中。

- 不停轮换与目标最近的监视人员或车辆，以减少目标察觉有人跟随的风险。（轮换是有规律的，且车辆有限。所以，平日多练习一些观察和记忆的能力，会很有用。□延伸：超强记忆力系列）

[image]

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

移动物理监视可通过以下方式实现：

- 在目标的车辆或自行车上安装追踪装置。
- 通过与移动网络运营商合作，获取目标手机的实时地理位置。
- 空中监视，例如无人机从远处跟随目标。

延伸：https://iyouport.substack.com/p/1200?utm_source=publication-search

延伸：https://iyouport.substack.com/p/150?utm_source=publication-search

[image]

返回：[image]你的手机如何背叛了民主？

静态

静态物理监控是指在目标无法移动或监控人员无意跟随其移动时对目标进行观察。静态物理监控行动通常由监控团队使用一辆或多辆车辆进行。

静态物理监控行动的示例包括将监控车辆停在目标住所前，监控人员在车内观察住所入口。类似于发生在中国的“上岗”监视。

逮捕

通常，监视团队在进行秘密物理监视行动时不会试图逮捕目标。不过也有极少数特例，如果监视团队已收集到足够关于目标活动的证据以证明其有罪，并认为有必要立即逮捕目标（例如为了在其关键行动之前直接阻止目标），这种情况可能会发生。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
✍️

笔迹分析

笔迹分析（也称为笔迹识别）是对笔迹样本的分析，通常用于将一个样本与另一个样本进行匹配，以鉴定其是否属于同一人。

[image] 一些银行抢劫案的实施方法是，悄悄地向出纳员递上索要钱财的书面纸条，以尽可能不引起注意。图中就是两张这样的纸条。注意其中的“0”字的写法，是一致的。

影响笔迹的因素

当您写字的时候，会自然地采用一种相对独特的笔迹，这主要取决于以下几个因素：

- 您是如何学习写字的：如何学习字体和笔画。
- 您的书写习惯：您的书写习惯与您学习写字的方式或多或少有关。
- 您的书写水平：是刚开始学习还是有经验的书写者。
- 书写工具：钢笔、铅笔、毛笔、喷漆罐、粉笔、板刷、湿苔帚等等。
- 操作书写工具的方式：右手、左手、脚、嘴、假肢等。
- 握住书写工具的方式：例如观察一下，当您写字时，笔放在哪根手指上。

- 书写在哪种表面：纸张、布料、混凝土等。
- 您写字时的姿势：坐着、站着、蹲着等。
- 书写环境：例如，您是否戴着手套写字、或在行进的车辆上写字。
- 书写时的身体和心理状态：疲劳、压力、因酒精、药物或成瘾物品（包括过量的咖啡因）引起的异常状态等。

分析

对手可以分析书写样本以识别其特征，包括：

- 文本布局：边距、行间距和行平行度。在信封的情况下：信封上地址的样式、大小和位置。
- 书写风格：例如，草书还是楷书。
- 字间距/单词间距。
- 单字/字母之间的连接或分离。
- 字体设计与构造：单字/字母的形状、单字/字母在样本中是否以一个或多个不同形状表示、不同形状的书写顺序、具体形状是否及如何受其前后其他形状的影响，以及形状的大小。
- 落笔和收笔的姿态，包括笔画长度、方向、路径和突兀程度。
- 书写工具对书写表面施加的压力。

- 书写工具相对于书写表面的位置。

在某些水平书写的语言中，对手还可以识别以下特征：

- 基线是否笔直或在样本中是否有所变化。（基线是单字/字母“坐落”的水平线。例如小写字母“p”的“小肚子”位于基线上，其“长尾巴”则延伸至基线之下。同样，“中”的口字位于基线上）

- 书写倾斜度：字体相对于基线的倾斜方向。

对手可通过比较书写样本与另一样本的特征，判断样本是否由同一人书写，并评估该判断的可信度。这一比较可由人类进行，也可以使用专用软件完成。

手写样本数据库

部分国家政府拥有手写样本数据库，可将样本与数据库中所有样本进行比对。例如，在美国，联邦调查局（FBI）维护着银行抢劫案记录文件（BRNF），其中就包含手写笔记样本。

推荐书目

相关详细介绍请参见《笔迹鉴定：事实与基本原理》一书。这是**Tor**链接，请使用**Tor**浏览器访问。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

警卫

保安人员是受雇于您的对手以保护某个特定建筑物或其他物理基础设施的人员。

如果保安在他们负责的区域内发现未经授权的入侵者，他们可以选择自行干预或请求外部援助。根据具体情况，他们可能配备致命的或非致命的武器。

📌 对应的镇压战术：逮捕

自卫措施

镇压行动案例

[image]

匿名购买

匿名购买顾名思义就是，在购置与您的敏感行动有关的物品时（包括支付相关的服务时）避免暴露真实身份的一些方法和原则。

举例比如：

- 如果镇压者在行动现场发现这些物品（例如，失效的延时燃烧装置）、或者这些物品的痕迹（如 纵火 取证过程中在现场附近发现的助燃剂痕迹），并且顺藤摸瓜发现了这些物品的购买地点，他们也不会查找到您的身份。

- 如果镇压者与银行系统合作获取了您的购买记录，他们也不会发现您购买了与某些行动相关的东西。

- 以及更多。

实体店匿名购买

要在实体店匿名购买商品，请记得：

- 提早买，不要临近用的时候再买。比如提前几周或者几个月购买。的确很多监视摄像头可以回溯查看，但不容易保存太久之前的影像。提早购买可减轻被回溯的可能性，即便被拍摄到。

- 不要在您的住所、工作单位、学校附近购买敏感物资。离远

点，越远越好。

- 使用匿名交通工具去商店，比如私人自行车、滑板车等（返回 [image]自行车接力 ）。并且，不要带手机、手表等电子设备。

- 在去商店之前采取主动的 [image]反监视 做法。

- 使用某种程度的 [image]匿名着装 原则来降低辨认度——“Covid”口罩、帽子、专用服装（比如您需要购买断线钳，穿得看起来像个工地工人或者消防员更好一些，而不是看起来像个老师）。

- 用现金支付。

- 与收银员的互动越简单、越普通越好。避免留下特别印象。

- 如果您需要购买多件商品，可以在不同的商店、不同的地点、不同的时间购买。一起买可能会引起怀疑，这一点尤其重要。

数字匿名购买

可以使用加密货币进行数字匿名购买。

您应该以匿名方式获取加密货币，或者在使用前对其进行充分清洗，这可能会比较麻烦，但对于像门罗币这样的加密货币，使用 Tails 是可以实现的。

顺便说，购买VPN也应该采取匿名购买原则，否则您的‘免追踪’措施很可能因购买而变得‘易追踪’了。

[image]

返回：[image]8个步骤实现基本匿名实践：变得难以被追踪的简单方法 S03E09

此自卫措施用于应对的镇压手段

[image]
□

DNA

DNA取证，是通过收集、存储和分析DNA痕迹，以便与个人身份进行匹配的工程。

[image] 中国城市的部分公共卫生间小便池。

收集

DNA是含有生物遗传密码的分子。除了红细胞外，人类身体的每个细胞都含有DNA。每个人都在通过皮肤细胞、头发、唾液、血液、汗液等不断将DNA释放到环境中。

DNA痕迹可以从人体或环境中收集，并在专业实验室中进行分析，以揭示其来源个体的相关信息。

□

延伸：https://iyouport.substack.com/p/-dna-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/66a?utm_source=publication-search

延伸：https://iyouport.substack.com/p/1e8?utm_source=publication-search

[image]

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法

S03E06

返回：[image]了解防暴弹药，以及如何保护自己 ：示威参与者指南 S05E10

分析

对DNA痕迹的分析可提供其来源个体的基本信息，例如遗传性别。通过比较两份DNA痕迹，可确定它们是否来自同一个体、是否是具有密切遗传关系的个体（如直系或旁系亲属）或无关个体。

环境中的DNA会随时间和特定条件而降解，进行DNA痕迹分析必须含有足够量的未降解DNA才能成功。随着技术进步，所需**DNA**量在不断减少。

在审判中，DNA经常被视为“黄金标准”，是证明某人曾接触某物/或身处某处的“无可争议的证据”。

DNA数据库

许多国家都拥有包含大量个人遗传信息的DNA数据库，这些信息通常在逮捕过程中或作为刑事定罪的一部分获取。有些国家/殖民地甚至强行收集。

推荐书目

《Dna You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces》，对DNA法医学文献进行了全面概述。

DNA You Say?Burn Everything to Burn Longer: A Guide to Leaving No Traces

https://www.notrace.how/resources/download/blabladn/dna-you-say-read.pdf

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

https://www.notrace.how/resources/download/rauber-und-gendarm-eine-geschichte-uber-ermittlungsmassnahmen/cops-and-robbers-a-history-of-investigative-techniques-read.pdf

[image]

痕量证据鉴定

痕量证据是指在物体、人员和环境之间转移的微小物理证据碎片。痕量证据可以通过收集和分析来建立物体、人员和地点之间的关联。

痕量证据可以是：

- 物质碎片。例如，鞋底上的泥土、或破碎窗户上的玻璃碎片等等。
- 当两个表面接触时留下的痕迹。例如，泥土中的鞋印、或断线钳在栅栏上留下的切口，等等。

痕量证据可以通过以下方式转移：

- 接触转移。例如，衣物接触围栏时，衣物上的纤维转移到围栏上。
- 非接触转移。例如，窗户破碎时，玻璃碎片飞散，细小的碎屑可能沾到附近人员的衣物上。
- 通过一系列的转移，包括有接触的也包括无接触的。

对手可以利用痕量证据：

- 分析行动现场的痕迹以获取有用信息。例如，对手可以分析行

动现场发现的鞋印，确定留下鞋印的鞋子的大小和型号，然后寻找拥有该大小和型号的鞋子的人。

- 将行动现场的痕迹与物体相关联。例如，对手可以确定在行动现场围栏上发现的纺织纤维是否可能来自他们在搜查您家时扣押的衣物。

- 将物体的痕迹与行动现场关联。例如，对手可以确定在您被捕时所穿的衣物上发现的玻璃碎片是否可能来自附近最近被打破的窗户。

- 将不同行动现场的痕迹关联起来。例如，他们可以确定在不同行动现场发现的锤击痕迹是否由同一把锤子造成的，因此这些行动很可能由同一群人实施。

痕量证据不包括指纹和DNA，后者被视为独立的法医学领域。

[image] 在显微镜下的观察（放大倍数约75倍），喷漆液滴附着在夹克衫的纤维上的样子。活动家经常会使用喷漆罐进行涂鸦，喷涂时产生的雾状油漆液滴很可能会落在附近的表面上，包括绘图者的衣服表面。其他行动现场所需物资也大多会留下类似痕迹。这就是为什么建议您撤离时更换衣服的另一部分原因。

纤维

由纺织纤维制成的物体（如衣物、包等）接触其他物体表面时，可能会在表面留下纤维。物体在表面留下纤维的可能性及纤维数量取决于物体本身、表面特性以及两者接触的时间长短和方式。

由纺织纤维制成的物体可能留下更多或更少的独特纤维，这取决于物体及其制造工艺。

例如：

- 一件颜色罕见且以罕见方式制造的旧羊毛衫，可能留下大量相对独特的纤维。

- 一件颜色常见、采用常见工艺制造的新尼龙风衣，可能不会留下任何纤维，或仅留下非常普通的纤维，无法与具体身份相关联。

对手可以做到的是：

- 分析纤维，以确定留下纤维的物体类型，在某些情况下还能确定其品牌和型号。

- 将纤维与持有这类纤维的物体进行比较，以确定某个物体是否可能留下这些纤维。

- 比较两组纤维样本，以确定它们是否可能由同一物体留下。

推荐文献

参见《痕量证据分析手册》，“纤维”章节，以了解纤维的概述。此处为Tor网络链接，请使用Tor浏览器打开。

脚印

当您赤脚行走时，脚与地面接触会留下脚印。您通常会在所穿鞋子的鞋垫上留下脚印。穿袜子时也可能留下脚印。

脚部可能留下或多或少独特的印记，这取决于脚部形状和接触表面的类型。例如：

- 在坚硬、多尘的表面上，脚部可能留下非常独特的脚印，显示出脚趾的纹路，这些纹路与指纹一样独特。

- 在柔软的表面（如沙地）上，脚部可能留下非常普通的脚印，仅显示出脚部的粗略轮廓。

对手可以：

- 通过分析脚印，以获取留下脚印的人的信息，例如脚的大小、身高估计、以及留下脚印时正在做什么 —— 站立、行走、奔跑、转身等。

- 将脚印与脚进行比较，以确定脚印是谁留下的。

- 将两个脚印进行比较，以确定它们是否由同一只脚留下。

推荐文献

参见《法医调查中赤脚脚印的检查与解读》，以获取关于脚印的概述。

鞋印

当您穿着鞋子行走时，脚底与地面接触会留下鞋印。

鞋印可能具有一定的独特性，这取决于鞋子的类型和接触的表面。即使是同一型号的批量生产的鞋子，由于制造过程中的不规则性和磨损模式，也会存在细微差异。例如：

- 在干净的木地板上，一双磨损且脏污的鞋子可能会留下非常独

特的鞋印。

- 在地毯上，一双新的、干净的、干燥的鞋子可能不会留下印记，或者只留下一个非常普通的印记，以至于难以追溯身份。

对手可以：

- 通过分析鞋印以确定鞋的大小型号，并获取留下鞋印的人的信息，如脚的大小和身高体重估数。

- 将鞋印与警方持有的鞋子进行比较，以确定这只鞋子是否留下了该鞋印。为此，他们可以用这只鞋子留下参考印记，并将其与可疑鞋印进行比较。

- 比较两个鞋印，以确定它们是否由同一双鞋子留下。

推荐文献

《鞋印证据：检测、采集与分析》这本书中有关于鞋印的全面概述。此处为**Tor**链接，请使用**Tor**浏览器打开。

工具痕迹

工具 —— 如钳子、剪刀、锤子、螺丝刀等 —— 会在被使用的物体上留下痕迹。

工具留下的痕迹可能具有更多或更少的独特性，这取决于工具类型、使用方式以及表面特性。即使是同一型号的批量生产的工具，由于制造过程中的不规则性和磨损模式，也会略有差异。例如：

- 一把磨损的金属锤子用力敲击由较软的金属制成的金属板时，可能会留下非常独特的痕迹。
- 一把全新的断线钳用于切割围栏时，可能会留下相对普通的痕迹。

对手可以：

- 分析痕迹以确定留下痕迹的工具类型。
- 将痕迹与警方获取的工具进行比较，以确定该工具是否留下了该痕迹。为此，他们可以使用该工具创建参考型痕迹，并与可疑痕迹进行比较。
- 比较两个痕迹以确定它们是否由同一工具留下。

推荐书目：

- PRISMA，“工具痕迹”章节，对工具痕迹的简要讨论。
- 《法医工具痕量识别彩色图谱》中有对工具痕迹的全面概述。此处为**Tor**链接，请使用**Tor**浏览器打开。

玻璃

当玻璃破碎时，会产生各种大小的碎片。

玻璃制品（如窗户、瓶子）在破碎时会产生更多或更少的独特碎片，这取决于其制造方式、地点和时间。

例如：

- 两种不同型号的玻璃制品，或在不同工厂制造的玻璃制品，或在同一工厂相隔数周制造的玻璃制品，其碎片可能通过分析其性质来区分（包括折射率和化学元素）。

- 两件相同型号的玻璃制品，在同一工厂同一周内制造，可能产生无法区分的碎片。

对手可以比较两片玻璃碎片，以确定它们是否来自同一物体。

推荐文献

《痕量证据分析手册》，“玻璃证据的解读”章节。此处为**Tor**链接，请使用**Tor**浏览器打开。

助燃剂痕迹

助燃剂痕迹在“纵火”页面中有所涉及。

其他

其他类型的痕迹证据包括：

- 人类和动物的毛发。毛发可能在任何时候从物体上脱落。毛发可揭示其所有者的各种信息，包括某些情况下的DNA。参见《痕量证据分析手册》- “法医毛发显微镜”章节，以获取关于毛发证据的概述。此处为**Tor**链接，请使用**Tor**浏览器打开。

- 涂料。涂有涂料的物体可能在接触的表面留下涂料的痕迹。涂料痕迹可揭示留下痕迹的物体相关的信息。参见《痕量证据分析手册》-“涂料与聚合物”章节。此处为**Tor**链接，请使用**Tor**浏览器打开。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

视频监控

大规模视频监控（即大规模CCTV监控网络）是指对来自视频监控摄像头的视频和音频数据进行大规模收集、存储和分析。旨在捕捉经过某个空间的所有人员身份，并将其覆盖范围扩大到尽可能广阔的区域。

如今一些国家的监控摄像头数量甚至超过了人口数量。

延伸：https://iyouport.substack.com/p/lr--a15

延伸：https://web.archive.org/web/20201027144114/https://www.iyouport.org/%E4%B8%AD%E5%9B%BD%E5%90%9160%E5%A4%9A%E4%B8%AA%E5%9B%BD%E5%AE%B6%E5%87%BA%E5%8F%A3ai%E7%9B%91%E6%8E%A7%E6%8A%80%E6%9C%AF/

https://iyouport.substack.com/p/lr--a15?utm_source=publication-search

数据采集

CCTV视频数据的来源包括：

- 街道或其他公共场所的监视摄像头。
- 私人建筑物内的监视摄像头（如商店、办公室等）。

- 公共交通工具上的摄像头（如公交车、火车、高速公路等）。
- 家庭监控系统，如亚马逊Ring等等。□ 延伸：https://iyouport.substack.com/p/e6d?utm_source=publication-search
- 车载监控系统，如特斯拉汽车上的系统。□ 延伸：https://iyouport.substack.com/p/d21?utm_source=publication-search

CCTV摄像头的质量、范围、夜视能力、是否配备麦克风等特性差异显著。

存储

采集后的监控录像通常会存储一段时间（从数天到无限期不等）。

□

延伸：https://iyouport.substack.com/p/a19?utm_source=publication-search

分析

监视者可以分析监控录像：

- 若摄像头集成到中央网络，可进行实时分析。实时分析可作为常规监控的一部分，或在特殊事件（如示威活动）期间进行。
- 若监控录像已被存储，可进行事后分析。事后分析可通过面部、步态、声音等特征识别目标人。

延伸：https://iyouport.substack.com/p/-192-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/f38?utm_source=publication-search

CCTV录像的分析可通过以下方式进行：

- 人工分析。
- 自动化系统分析，如自动车牌识别系统或人脸识别系统。

延伸：https://iyouport.substack.com/p/lr--bc3?utm_source=publication-search

延伸：https://iyouport.substack.com/p/c9e?utm_source=publication-search

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]
▯

告密者（线人）

线人（或告密者）是指被对手招募的、来自某个群体或网络内部的人员，其任务是向对手提供该群体或网络的相关信息。

渗透者来自外部；线人来自内部。

[image]
[image]

返回：本站专题栏目《反渗透、减轻背叛，和协作》

对手可以采用不同的策略来招募线人：

- 针对那些被认为更可能成为线人的人群：比如，在具有等级制度的群体/圈子里长期被排挤而处于边缘的人；战略模糊/政治理解能力较差的成员；因各种可能的内部纠纷而离开某个群体/圈子且心怀怨恨的人……
- 以负面后果威胁拒绝成为线人者：更长的监禁刑期、驱逐出境等等…… 取决于被威胁的人被认为的'最大恐惧'所在。国家对社会的控制手段越多，可用的威胁手段就越多。
- 以正面后果诱使成为线人：在被要求成为线人的司法案件中获得豁免或宽大处理，或者在其他案件中获得金钱奖励…… 取决于被威胁的人被认为的'最大需求'所在。

对手可以利用线人收集证据以定罪目标人、和/或绘制一个行动群体的关系网结构（连锅端）。

📌 对应的镇压战术：指控。

[image] [image] 原文：https://t.me/iyouport/13902

自卫措施

镇压行动案例

[image]

DNA最小化方案

尽量少地残留DNA，同时不影响计划中的行动。

有些方案专注于从一开始就不在物体上留下 DNA 痕迹。另一些则专注于通过化学方法破坏 DNA 分子，从而去除物体上的 DNA 痕迹。

DNA最小化方案可能涉及：

- 购买单独塑料包装的物品，这样在打开包装之前就不会有 DNA 残留的风险。
- 戴着一副新的非渗透性手套（例如洗碗手套）操作物体，这样手套外面就不会有 DNA 痕迹转移到物体上。
- 将物体存放在新的、不透水的垃圾袋中，这样环境中的 DNA 就不会在存储过程中污染物体。
- 用次氯酸钠破坏 DNA 分子，某些品牌的漂白剂中含有足够浓度的次氯酸钠。

推荐相关知识资料

- 《DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces》

- 《Minimizing DNA Traces During Riotous Moments》

此自卫措施用于应对的镇压手段

[image]

渗透者

渗透者是指通过伪装成他人身份，渗透进入某个团体或网络，以获取情报、和/或为了破坏该团体或网络稳定的人。

渗透者可能来自警察、情报部门或军队，也可能来自私营公司或承包商，还可能出于意识形态原因或者被胁迫（例如，他们被国家机器告知如果不以渗透者的身份行事，就会被监禁）。

[image]

返回：本站《 反渗透 》专题栏目。

强调：没有任何一个或几个特征能百分百确定渗透者；错误指认的结果可能比渗透本身的危害更大。您能做的最好的防御就是令渗透计划不起作用；绝不是抓特务，因为永远都不可能“清除”所有渗透，除非您和您的团队永久性地失去行动力和影响力，被困在恐惧中。

加强自身，是唯一的办法。我们的目标应该是：努力建立一个更安全、更难以渗透的网络。

有五种基本的渗透者类型：

1. 闲逛者： 很少参加真正的行动，只热衷于参加各种会议、社交活动、收集文件、观察和倾听。

1. 沉睡者： 起初非常低调，几乎不可见，在某一事件/事态下忽

然变得非常活跃。

1. “马仔”人设： 政治分析能力很低，倾向于跟随别人，甚至只是吹捧和模仿圈子里看起来有权威的人；长期致力于为自己建立信任和信誉（对被信任不足非常敏感）。由于跟圈子权威人物的私人关系热络，更容易实施挑拨和拉帮结派。这种情况尤其容易出现在等级制度明显的圈子中。换句话说，这样的人致力于搞关系，而不是搞志业。

1. ‘超级’活动家： 几乎无处不在，同时加入多个团体或委员会，作为组织者。跟普通积极分子不同的是，这种“超级”活动家几乎不会对项目的进展起到作用，相反他们更热衷于笼络权力和人心。

1. 极端激进者：经常不合时宜地主张激进行动和暴力冲突。请注意“暴力/非暴力”不是道德问题，而是战术有效性问题；“不合时宜的暴力”主张就是战术有效性为零，而被抓捕的可能性百分百：https://iyouport.substack.com/p/ad0?utm_source=publication-search

---

渗透可“浅”可“深”。浅层渗透者可能持有假身份证明，但更有可能在周末回归他们自己的正常生活。浅层渗透通常发生在情报收集周期的早期，一定程度上这一阶段仍然处于对目标的识别过程中。

相比之下，深度渗透则需要24小时全天候工作，并且持续很长时间（期间也可能会定期休息）。他们可能拥有一份工作、一套公寓、一个伴侣，甚至一个家庭，作为渗透的一部分。他们会使用政府签发的假身份证件、工作经历和租房记录等。

延伸：https://iyouport.substack.com/p/f2f?utm_source=publication-search

[image]

返回：[image]别再瞎抓‘特务’了：创建更安全的关系网络的指南 - 关系结构革命S11E01

📌 对应的镇压战术：指控。

自卫措施

[image]

返回：[image]草木皆兵和”爱谁谁”都只会带来更多的危险：整体安全S01E06 - 开发您的能力，缓解您的脆弱性

镇压行动案例

[image]

道路封锁

道路封锁是为了控制或阻断特定道路的交通而设置的临时设施。

镇压者设置道路封锁，是为了：

- 作为一项有计划的措施，例如在已知将要发生抗议活动的街道周围，控制抗议者的流量。
- 临时围堵，例如在某项行动之后镇压者想要抓住参与该行动的人。

在某些情况下，警方会在某些事件发生后系统地设置路障，例如引人注目的抢劫案或越狱事件。

自卫措施

镇压行动案例

[image]
🎯

有针对性的数字监控

定向数字监控是指对数字数据和通信进行有针对性的收集和分析。

国家行为体拥有极为先进的监控技术这是众所周知的，不过本页面重点讨论的是更可能被用于针对无政府主义者和其他反叛者的监控技术。

📌 对应的镇压战术：指控。

5个子项目

[image]
[image]

身体暴力 (含酷刑)

身体暴力是指对手通过使用武力来威吓目标或其关系网、使目标失去行动能力，或迫使其透露信息。

身体暴力包括酷刑，且不限于。例如，在俄罗斯和白俄罗斯等国家，近年来有多名无政府主义者在被国家逮捕后遭到酷刑。这些国家报告的酷刑手段包括：殴打、用塑料袋或枕头窒息、往鼻孔和嘴里灌水、倒挂双腿或绑住双手、电击、用螺丝刀施刑、强迫做深蹲直到筋疲力尽倒下、性暴力，以及剥夺睡眠、食物和水。

在某些情况下，身体暴力也可能包括暗杀。

[image]

返回：[image]为最坏的情况做准备，迎接最好的结果如何在敌对环境中保护自己S02E04

□

延伸：https://web.archive.org/web/20250601034455/https://iyouport.substack.com/p/342

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]

掩盖写作风格

掩盖您的写作风格是通过改变您的写作方式来对抗法医语言学 - [image]语言指纹 。

例如：

- 您可以简洁而有目的地写作。 取消所有铺陈，越简单越好。
- 在发布文本之前进行详细的检查，以确保其中不回包含任何可以追溯到您身上的独特错误（错别字、习惯性的缩写、标志性口头禅等等）。
- 为了识别某人是某个文本的作者，镇压者通常会搜罗大量该人曾经写作的样本进行比较。为了避免这种情况，请不要在家中保存没有加密的写作样本，以免在[image]隐蔽性地突袭住所或抄家 时被发现 ，并且，您应该始终不要完全以真实身份发表文本 —— 匿名写作值得贯彻一生。

推荐反制法医语言学的材料：

[image]

注：中文文档为AI翻译的结果。我们还没有时间进行具体校对。诚邀有能力的朋友进行详细编译。如果您有意，欢迎联系我们。

- Who wrote that?
  反制法医语言学.pdf

此自卫措施用于应对的镇压手段

[image]

反攻

常言说得好，最好的防御就是进攻。

其实这里的“反攻”也可以称为“进击”，因为它不一定必须是被动的 —— 不是在被打击后的反弹，它完全可以是主动的 —— 先下手为强。

Apple TV+ 有一部剧集名为《德黑兰/Tehran》，其中有一个情节，伊朗反对派团队内有专门的黑客，在行动之前先入侵监视系统，关闭行动路线上所有监视摄像头。这种做法就是主动的反攻。并且不需要如此高技术门槛，2019年香港的抗议者推倒“智能灯柱”监视器的行动也是一种主动反攻。

https://youtu.be/BzQoMAH3yLo?si=INzGkIbbrnJ_8jRy

顺便说，香港的行动例子不是太好，因为它执行困难，难度成本与阻止监视的目标收益不成比例。但作为示威行动的一部分它是很有景观价值的。而本页话题期待的“反攻”行动的有效性高于景观价值。

比如，告密者（线人） 和 渗透者 如果被吓到，他们的行为就会有所收敛。您的小心翼翼并不足以抵制渗透破坏，您需要反攻。

再比如，某个地方警力增加，意味着其他地方警力减少。如果您的项目重点在于B地点，那么A地点就可以用来吸引维稳资源。

再比如，警察的通信和调度依赖地面集群无线电(TETRA)和P25，警务行动的顺利进行则取决于车队、警站以及警员个人的安全感，所以现在您知道了……

[image] [image]

想象力和创造力至关重要！

此自卫措施用于应对的镇压手段

[image]
🎭

面部识别

面部识别是对人脸特征的分析，以便确认身份。

人脸识别技术是指通过人工或自动系统定位并测量人脸（或人脸图像）的特征（如鼻子的形状、眼睛之间的距离），并将这些特征与另一张人脸（或人脸图像）的特征进行比较。如果两张人脸的特征足够相似，则认为这是同一个人。

现代人脸识别系统能够将人脸图像与大型人脸数据库进行比对，即使图像中的人脸被部分遮挡，仅露出眼睛和眉毛也能实现匹配。人脸识别系统与大规模视频监控相结合，可用于自动追踪个体在空间中的移动轨迹。

延伸：https://iyouport.substack.com/p/lr--bc3?utm_source=publication-search

延伸：https://iyouport.substack.com/p/f18?utm_source=publication-search

延伸：https://iyouport.substack.com/p/5-7c3?utm_source=publication-search

延伸：https://iyouport.substack.com/p/833?utm_source=publication-search

延伸：https://iyouport.substack.com/p/bb9?

utm_source=publication-search

延伸：https://iyouport.substack.com/p/--ba5?utm_source=publication-search

📌 对应的镇压战术：指控。

[image] 以防晒为名合理合法的遮挡似乎正在被更多人采取。不过要提醒的是，这种方法只适合日常 **[image]** 生物特征隐藏 ，街头实战则不建议，因为面对警方防暴武器时它没有抵抗力。 BACK

自卫措施

镇压行动案例

[image]

背景调查

背景调查用于验证一个人的身份是否与其声称的身份相符。这是一个检验步骤，用以分析您的合作网络中的某个人是否渗透者、告密者，或出于恶意目的谎报身份。

对某人进行背景调查可能涉及：

- 联系或会面他们的朋友或家人，询问有关他们的事。
- 拜访他们的家或工作地点。
- 查询关于他们的身份或行政文件（就业或租赁历史、犯罪记录等等）

建议采用两种不同的背景调查方法：

- 双方同意的相互方法：如果您已经在某种程度上信任某人，但希望更加信任他们，那么你们可以进行相互背景调查，即互相检查对方。
- 非自愿方法：如果您已经强烈怀疑某人在谎报身份，您可以在未经其同意的情况下对其进行背景调查，以证实您的怀疑。

推荐以下书目

[image]

注：中文文档为AI翻译的结果。我们还没有时间进行具体校对。诚邀有能力的朋友进行详细编译。如果您有意，欢迎联系我们。

- Confidence, Courage, Connection, Trust - A proposal for security culture
- Handbook for Exposing an Undercover Cop
信心、勇气、联结、信任 - 安全文化提案【AI版】.pdf
揭露卧底警察手册【AI版】.pdf

此自卫措施用于应对的镇压手段

[image]
🚨

报警系统

报警系统是通过在检测到对基础设施的未经授权访问时发送警报信号来保护物理或数字基础设施的机制。该警报信号可触发安保人员或执法部门的快速介入。

对于物理基础设施，现代报警系统通常包含可在非正常工作时间检测到对特定区域的未经授权访问的传感器。此类传感器包括红外线运动探测器、检测门开启的传感器、以及其他多种类型的传感器。警报信号可通过有线或无线连接发送 —— 低成本的现代报警系统常通过移动通信网络发送信号。

对于数字基础设施，入侵检测系统会监控任何可能表明正在发生黑客攻击的活动。若检测到未经授权的访问，可通知事件响应团队尝试遏制并修复任何安全漏洞。

📌 对应的镇压战术：逮捕

[image]

返回：[image] “智能城市”究竟是个什么鬼

自卫措施

[image]
👂

窃听

通常是麦克风，用于收集音频数据。

延伸：https://web.archive.org/web/20250202145335/https://iyouport.substack.com/p/bdc

延伸：https://web.archive.org/web/20250202150800/https://iyouport.substack.com/p/a7b

延伸：https://web.archive.org/web/20250202150543/https://iyouport.substack.com/p/lr--53c

延伸：https://web.archive.org/web/20250202145021/https://iyouport.substack.com/p/lr--1c6

对手可以在任何可能收集到有价值音频数据（通常是对话）的地方隐藏音频监听设备。

值得注意的地点包括：

- 目标人住所的客厅。
- 目标车辆的仪表盘。

- 目标经常与他人会面或预计会面的户外地点。

隐蔽的音频监听设备非常敏感，即使在背景有较大噪音或目标人窃窃私语的情况下，也能成功捕捉到对话。窃听器可以非常小 ——仅几毫米—— 尤其是那种在本地记录（例如在SD卡上）不传输录音的窃听器。

录音内容若涉及定罪证据或可被歪曲解读为证据，便很可能在法庭上作为证据使用。就连最普通的日常对话也能揭示被监视对象的诸多信息，并有助于构建目标人的社交网络关系图谱，有利于连锅端。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

反监视

反监视是指采取主动措施规避监视行动的做法。中文俗语叫“甩掉尾巴”。

[image]

返回：[image]监控侦测

何时进行反监视

有两种情况，且只有这两种情况，您应该进行反监视：

1. 如果您正前往执行某项不希望被对手察觉的行动，且未发现遭人尾随的迹象，可实施反监视，以规避潜在的监视行动。此情境下实施反监视的目标是：最大限度地降低执行此次计划行动时遭尾随的风险。

1. 如若存在被跟踪迹象，且怀疑对手正计划立即对您采取暴力行动（如逮捕或袭击），则应实施反监视。此情境下实施反监视的目标是：规避可能的暴力行动。

其他情形则不应实施反监视行动，原因如下：

1. 如果您正前往执行不希望被对手察觉的行动，但发现遭尾随迹象，您无法确证所采取的反监视措施是否能成功摆脱监视。因此无论如何都将取消计划中的行动，反监视行动就没意义了。

1. 如果察觉遭尾随，但没有怀疑监视方计划立即采取暴力行动，实施反监视反而会暴露您察觉到了尾随，可能促使对手调整策略并采取更隐蔽的行动方式 —— 这叫打草惊蛇，正是您需要避免的。

核心原则

反监视的核心原则在于：通常对手的监视行动极不愿被目标察觉，宁可跟丢了也不想暴露监视者的行踪。因此，您采取的大多数反监视措施都应试图引发两种情况之一：要么让监视者暴露行踪以便您侦测，要么迫使他们放弃跟踪。实施反监视措施时需保持警觉，以便发现因此暴露身份的监视者。

示例

反监视属于高级操作。实施前建议通过下面的链接进行相关学习。

暗网：http://sx3kelhcum7aaemtp27n2p3x4figvaymt2vibcabjpftxupzuu5ifzyd.onion/#surveillance-countermeasures

延伸：https://www.notrace.how/resources/download/massnahmen-gegen-observation/measures-against-surveillance-read.pdf

具体反监视手段包括：

- 进入监控行动的“盲区”—— 即监控方无法看见您的空间，随后实施一系列规避动作，同时持续侦测监控人员。例如在城市街头步行时，可快速进入拥挤的公共建筑，然后迅速从后门离开，再继续规避动作。若发现有人在您之后匆忙进入建筑，或

在您离开后在街上搜寻您的踪迹，他们很可能是就是监视者。

- 从开阔区域（监控方需保持距离以避免暴露）转移至较封闭区域（监控方需靠近以避免丢失目标），同时持续侦测可能的监控方。例如在乡村骑行时，可从视野开阔的道路忽然转入林间小径，加速深入森林后从远离入口处出林—— 这正是监视者意料之外的路线。若进出林地时发现有行为异常的人，则可能是监视人员。

补充注意事项

若对手察觉到您正在实施反监视行动，他们可能调整策略并加强隐蔽性。因此进行反监视时，应尽可能避免暴露自身意图。

[image]

返回 - 反监视的心理技巧：[image]思考方式是战略性的：完美隐身 S04E03

[image]

返回：[image]特工战斗法帮你摆脱跟踪监视：反侦基础课 S06E06

返回：[image]警察通常会如何寻找一个"失踪的/躲起来"的人: 反侦基础课 S06E06A

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

返回：[image]如何检测您是否正在受到监视：监视检测和特殊保护

行动

返回：[image]暗中监视的迹象

此自卫措施用于应对的镇压手段

[image]
🚶

步态识别

步态识别是对人行走的方式或风格进行分析的过程，以便确认身份。

[image] 左图：一个人行走的侧面图。右图：同一个人行走的正面图。红线标记了一些用于步态识别的身体特征。

步态因素

当您走动时，您会自然地采用一种相对独特的步态，这种步态取决于多个因素，包括：

- 内在因素：您如何学会走路的、身体的解剖结构和生理特征，以及您可能存在的任何伤痛或病理状况。
- 外在因素：您的穿着（宽松还是紧身、遮住腿部的长款还是在腰部以上的短款、鞋子是否不合脚或款式不习惯）、以及您行走之处的地形（平坦与否，是否有障碍物等）。

延伸：https://iyouport.substack.com/p/72a?utm_source=publication-search

延伸：https://iyouport.substack.com/p/057?utm_source=publication-search

[image]

返回：[image]如何躲避无人机 - 监视时代须知

分析

通过观察您的行走，对手可以定位、测量并分类关于您在移动过程中不同阶段的身体特征（如脚踝、膝盖、髋关节的位置等），并将这些特征与另一个行走中的人的身体特征进行比较。这种比较可以让对手判断两个行走的影像是否可能是同一个人，但通常无法直接确定您的身份 - 除非对比影像中至少有一个是已知身份的。这种比较通常由人类进行，有时会借助专业分析软件。

步态识别通常通过比较两组视频片段来实现。每组视频显示一个目标人的行走。比较的目的是确定第一人和第二人是否可能是同一个人；以及可识别性强度，即确定第一人是否可能是第二人的信心程度。这取决于多个因素，包括：

- 视频片段的质量和帧率。
- 场景中的光线条件。
- 人体是否足够靠近摄像头、整个身体是否完全可见、是否能看到迈出多个连续的步子，且目标人穿着不会过度遮挡步态的衣物（比如格外宽大的衣服 - 袍子/风衣，都可能遮挡步态）。
- 两个目标人是否具有标准的或独特的步态。例如，跛行者具有较为独特的步态；军姿正步是标准步态。
- 两个目标人是否从相似的角度执行相同类型的动作（如行走或跑步）。

典型场景

以下是一个对手利用步态识别技术的典型场景：

- 某人被监控摄像头捕捉到正在执行某项行动。由于其穿着匿名，无法从外表被识别。于是对手获取了监控录像。

- 基于其他证据，对手怀疑某人实施了该行动。他们获取了该嫌疑人的活动录像，可能是通过其住所附近的监控摄像头、拘留期间的监控录像，或隐蔽的视频监控设备。

- 将第一段录像中该人的步态与第二段录像中嫌疑人的步态进行比较，以确定两人是否为同一人，并评估该判断的可信度。

推荐书目

《法医步态分析：原理与实践》，本书提供了关于步态识别的全面概述。此处为Tor链接，请使用Tor浏览器获取。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

警犬

警犬是经过训练以被用于检测气味的犬类。可用于检测爆炸物或毒品等物质、追踪目标人员，以及参与气味辨认程序以确定目标人的气味是否存在于某些物体上。

延伸：据报道，中国西南部云南省的科学家克隆了警犬，他们称之为“警犬中的福尔摩斯”，希望此举能帮助减少警犬的训练时间和成本。https://www.theguardian.com/world/2019/mar/20/china-clones-sherlock-holmes-police-dog-to-cut-training-times-report

气味是由物质释放的挥发性化合物引起的。例如，旧书的气味是由纸页不断分解时释放到空气中的化学化合物引起的。

人体气味，即所谓的体味，是由水分泌物（汗液）、油分泌物（皮脂）、皮肤碎屑和身体开口（如口腔、鼻腔等）释放的化合物引起的。每个人都有相对独特且随时间相对稳定的标志性气味。

犬类的嗅觉比人类的嗅觉复杂且发达得多。犬类可以：

- 检测非常微弱的气味。
- 在混合气味中识别单一气味。
- 判断气味来源的方向。

- 以极高精度感知气味强度。例如，若两种气味在相似条件下存在，它们可判断哪一种气味更强烈，从而推断其更近期。

检测物质

对手可以训练警犬来检测爆炸物、毒品、助燃剂、或较少见的电子设备等物质发出的气味。

对手可以使用警犬：

- 在行动现场或房屋搜查、秘密入户搜查时，确定某种物质是否存在，并定位其位置。

- 在身份检查时，确定被检查者是否携带或接触过某种物质。

在许多国家，国家机构会使用警犬在边境、机场、火车站等场所检测所谓的“非法物质”。

追踪人员

当人步行移动时，会留下由以下成分组成的气味轨迹：

- 其自身体味，包括脚部分泌的水分（汗液）和油脂（皮脂）气味，以及身体脱落的皮屑气味。汗液和皮脂气味会渗透鞋子，包括橡胶鞋。

- 附着于脚底或鞋底的物体的气味。

- 如果穿着衣服：衣服上脱落的颗粒的气味。

- 如果穿着鞋子：鞋子材料的气味（橡胶、皮革等）。
- 如果踩踏过活的植物，包括草：被踩到的植物释放的汁液气味以及破碎部位细菌分解的气味。
- 如果踩到的是小昆虫或其他小型动物，会带有动物尸体的气味。

对手可以训练警犬追踪此类气味的轨迹。

追踪方法有两种：

- 第一种方法：向犬只提供气味样本（例如嫌疑人穿过的衣物、摸过的东西），并要求其定位并追踪含有该气味的轨迹。此方法更可靠。
- 第二种方法：不向犬只提供气味样本，直接要求其定位并追踪轨迹。此方法可靠性较低。

在许多国家，国家机构使用嗅探犬追踪嫌疑人，但由于犬只被认为不可靠，追踪结果在法庭上不被视为有力证据。在某些国家，上述第一种方法的追踪结果被视为有力证据，而第二种方法的追踪结果则不被视为有力证据。

侦查犬通常可在气味痕迹留下后两至三天内跟随，甚至在某些情况下，根据不同因素，可长达两至三个月。

影响侦查犬在气味痕迹留下后较长时间内跟随能力的主要因素包括：

- 犬只及其训导员的训练水平。

- 人类在气味痕迹上或附近的活动（比如游泳过河、用很强烈的异味掩盖等等）。

- 风力。空气流动可能分散构成气味痕迹的挥发性化学物质。

- 降水。雨水、雪或露水可能溶解构成气味轨迹的部分挥发性化学物质。

气味排列测试

对手可训练警犬参与气味排列测试。

设置气味排列测试时，对手会从嫌疑人及另外5至10人处采集气味样本，并将样本并排放置于空旷房间内，确保样本之间保持一定距离。随后，向犬只提供一种目标气味，并要求犬只判断是否有任何气味样本与该气味匹配。

通常，犬只被提供在行动现场收集的疑似携带嫌疑人气味的物品：若犬只判断嫌疑人的气味样本与该物品的气味匹配，对手可推断嫌疑人曾接触该物品并可能参与了该行动。

气味辨认程序的结果通常不被视为法庭上的有力证据。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]

定位追踪

最常见的是微型蓝牙追踪器，类似苹果AirTag。更重要的是要记得，敏感时段不要使用联网汽车。

[image]

[image]您是否正在被 AirTag 跟踪？这里是检查方法

对手通常会将隐蔽的定位监控设备藏在目标常用的交通工具内部或外部，例如汽车或自行车。

隐蔽的定位监控设备通常通过以下方式实现定位：

- 最常见的是使用GPS。
- 在某些情况下，使用GPS的替代方案，如格洛纳斯系统(GLONASS)或卫星电话服务。
- 在极少数情况下，通过发射无线电波，由附近的监控操作员（通常在跟随目标车辆的监视车辆中）接收。

收集的位置数据可作为法庭证据。非指控性的、日常位置数据可用于揭示目标人的许多信息，并有助于映射目标的行动习惯和重要关系网络。

延伸：https://iyouport.substack.com/p/150?

utm_source=publication-search

延伸：https://iyouport.substack.com/p/d21?utm_source=publication-search

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

对证据的偏见性解读

对证据的偏见性解读是指以有利于特定观点的方式解释证据的做法。目的是定罪，甚至栽赃。

对证据的偏见性解读是现代司法体系的惯常做法，这种做法往往偏袒富人和权势者，而歧视反抗者和反叛者。

证据在各个环节都有可能被带偏见地解读：在调查人员收集证据时、检察官提交证据时，以及法官审理案件时。

这是一种叙事武器。任何信息 —— 包括日常信息 —— 都可以被编织成一个符合调查目的的故事。

▯

延伸：

[image]

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

自行车接力

就是说使用自行车替代其他交通方式。

是无主的大众款自行车，不是共享单车！也不是非常高档独特的自行车！

自行车的优点在于：

- 在视频监控的“眼中”，识别自行车比识别汽车更困难。
- 骑自行车的人更容易进行[image]监控侦测 和[image]反监视 行动，因为比其他交通工具都更灵活自如。比如法国的案例，警方对一名无政府主义者进行了为期6个月的物理监视，整个过程中目标人坐汽车和步行的状态都不如骑自行车时更难跟踪。警方经常在他骑自行车时跟丢。

此自卫措施用于应对的镇压手段

[image]

手套

手套可以防止在您触摸过的物体表面留下指纹和 DNA，并可以隐藏您的手部特征。

指纹和DNA

为了避免在触摸的表面留下指纹和 DNA，请使用合适的手套：

- 使用不渗透的厚乳胶手套或橡胶手套。
- 请勿使用薄手套（例如薄的乳胶或橡胶手套），因为薄手套掩盖指纹的效果差。
- 不要使用皮手套，因为它们会在您触摸的表面留下标志性的独特印记（称为手套印 ）。
- 不要使用普通的劳工毛线手套或布手套，会导致汗水渗透出来（即DNA泄漏）。

采取适当的预防措施：

- 确保您的DNA没有残留在手套外层，因为它可能会从手套转移到您接触的任何表面上。为此，您应该使用一副单独密封包装的新手套。

- 戴手套的过程要小心，避免DNA残留在手套外层。为此，请用裸露的手捏住另只手手套的内侧，然后把手戴进去，然后用戴着手套的那只手捏住另一只手的手套的外侧，再戴另只手套。

您也可以将多副手套叠戴。例如，在厚乳胶或橡胶手套外面再戴一副劳工手套，既能发挥劳工手套的坚固性（不容易刮破），又能兼具厚乳胶或橡胶手套的防渗透性。

手部特征

为了隐藏您的手部特征，例如肤色或纹身，请佩戴完全遮盖皮肤的手套。请参阅相关的缓解措施 [image]匿名着装 。

其他注意事项

- 请记得，根据手套的材质，您可能会在所戴手套的内侧留下指纹。

- 您戴的手套内侧会留下 DNA。

- 如果在行动中戴着手套，来自行动现场的痕迹（例如痕量助燃剂）可能会沉积在手套上，而手套的痕迹（如纺织纤维）也可能沉积在行动现场。这些痕迹可以用来将手套与行动现场联系起来。 BACK 痕量证据鉴定

由于所有这些原因，如果您在行动中需要使用手套，则应使用专用于该行动的全新手套，并在行动后将其销毁。

[image]

返回：[image]指纹

[image]

更多资源：https://web.archive.org/web/20250615110720/https://militanz.blackblogs.org/163-2/

此自卫措施用于应对的镇压手段

[image]

平民告密

是指不属于敌方侦查人员的随机平民，向敌方举报您。比如“自干五”、法西斯分子等等；或者因遭到警方问讯而提供了关于您的任何信息的“目击者”。

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]
🚔

增加警力

增加警力是指警察在特定时间和地点调动更多警力的过程，其原因有二：要么是为了威慑，要么是镇压战术的调整（接下来会有大动作的那种）。

增加警力的例子包括：

- 特定区域的警察巡逻更加频繁。
- 在公众示威活动现场部署更多的警力和车辆。在示威活动开始前的几个小时里，警力和车辆可能会聚集在示威活动周围或预期目标周围的街道上。这种聚集为警方在示威活动之前、期间和之后进行公开监视提供了机会。

📌 对应的镇压战术：逮捕、威慑。

自卫措施

[image]

公开监视

公开监视是指监视者打算被目标发现或不介意被目标发现时对人或活动的直接观察。这种做法在示威活动和集会中很常见，目的是确定参与者的身份，以便于绘制关系图谱、或者将示威期间的个人行为入罪。

[image]

返回：[image]如何识别抗议活动中可见的和不可见的监视

只对少数人进行公开人身监视的情况很少见，其目的往往是通过制造恐慌氛围来阻止统治者不喜欢的活动/行动，而不是为了定罪。

对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
□

恶意软件

恶意软件被安装在计算机、服务器或移动电话等数字设备上，旨在破坏设备的安全性。

□

延伸：https://start.me/w/8LRjvQ

恶意软件可以执行非常多不同的功能，但针对无政府主义者和其他反抗者时，其主要目标通常是通过远程屏幕捕获和远程键盘记录（记录键盘按键操作）来获取受感染设备的访问权限，并追踪设备的位置（在手机的情况下）。

[image]

返回：[image]如何检查MacOS上的恶意软件和键盘监听程序

□

延伸：https://iyouport.substack.com/p/nsa?utm_source=publication-search

延伸：https://iyouport.substack.com/p/4bc?utm_source=publication-search

延伸：https://iyouport.substack.com/p/as27-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/627?utm_source=publication-search

恶意软件可通过以下方式安装在设备上：

- 远程安装，通常通过钓鱼攻击（通过电子邮件或基于文本的消息，如短信等）。为了有效实施钓鱼攻击，通常需要目标用户主动点击恶意文件或链接。 BACK 返回：在本站“心理安全”专题中找到社交工程防御建议

- 通过物理访问设备，即恶意女仆攻击。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

敲门

对手直接来到您的住所并敲门，目的是为了威吓您，和/或获取信息。

敲门行动旨在通过威吓或制造忐忑的心理环境，以识别/引诱有可能透露信息的人，并可能将其招募为线人，同时从嘴巴不严的人那里 收集信息 。

并且敲门不是全部。接下来对手会记录您与敲门者通话或会面后立即联系的人是谁 —— 很大程度上那就是您最信任的人，甚至托付之人，从而可以绘制出你们的关键社交关系网络。

在许多国家，警察直接敲门比进行房屋搜查更容易，因为敲门不需要搜查令或法律授权。

📌 对应的镇压战术：威慑、指控。

自卫措施

特别注意事项

华语朋友都知道“查水表”是什么意思。欺骗性敲门是最常见的逮捕方式，警方可能声称一些不相关的事情要求您开门。而您一旦开门，就会被实施逮捕。在这种情况下警方没有“闯入”，是您“主动”开门的。

所以，不要随便开门。

2019年5月22日，意大利的反法西斯活动家波巴在家中被逮捕，警方敲门时只是声称“需要口头警告”。警方还对他的住所进行了搜查，没收了电子设备。在这里看到该案件。

[image]

户外无设备对话

户外无设备对话是指在户外不使用电子设备进行高度敏感对话的做法，以确保不被对手听到。

这里所说的“敏感”是指谈论可能直接定罪某人的话题。换句话说，保密事关人身安危。

户外和无设备是敏感对话的两个必要条件，因为：

- 室内空间（包括汽车里）都有可能被安装[image]隐蔽监视 设备。
- 电子设备可能会感染恶意软件 ，从而变成隐蔽的窃听器。

毫无疑问，本站大部分内容都在努力帮助您避免这类威胁，但必须承认，技术性防御有一定门槛，并且，只要您的对手有足够的资源（包括他们认为“值得”对您的项目耗费足够大的维稳资源），普通的防御措施都可能被挖到漏洞。最彻底的办法就是，直接避开可能存在威胁的地方。

请注意，监视者可以使用隐蔽麦克风或长距离抛物面麦克风录制户外对话（范围可达300米），属于[image]物理监控（上岗） 行动的一部分。

例如， 2019年在意大利，在一所经常举行集会的监狱门前，监视者在一块假石头里隐藏了窃听器。这真的是防不胜防的。https://www.notrace.how/earsandeyes/#cuneo-2019-06

因此，户外对话如果是少数私人交谈的话，建议你们边走边聊，不要停在某个地方；另方面，对于难以移动的大型群体对话来说，建议在经常变化且难以进行音频监控的空间进行。

最好将手机留在家中。法拉第袋并不能阻止音频被捕获，只能阻止音频被传输，而当手机稍后重新连接到网络时，音频传输可能会开始。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

此自卫措施用于应对的镇压手段

[image]
[image]

黄貂鱼

IMSI捕获器（也称黄貂鱼）是一种用于收集其周围有限区域（几米到几百米）内所有已开启的手机信息的设备。被动黄貂鱼仅监听流量，主动黄貂鱼则充当手机和合法基站之间的“伪”基站。

[image]

工具：[image]找信号：对抗黄貂鱼等监视设备

IMSI捕获器可以收集其周围手机的以下信息：

- 手机号码。
- 手机的IMSI和IMEI号码。
- 关于手机活动的相关数据和元数据：短信和普通通话的内容、访问过的网站列表、端到端加密消息应用程序的使用元数据（例如，当使用Signal时，以及通过Signal发送或接收的消息的大致大小）。 BACK 返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

□

延伸：Semptian的文件指出，Owlet 有能力同时监控200部不同的手机。“大规模拦截系统用于拦截覆盖范围内的所有语音和短信，”一份描述 Owlet 的文件说 …… 它被设计用于跟踪目标手机在近1英里半径范围内的位置，并可将其精确定位在5米范围内，与美国执法部门使用黄貂鱼的设备类似 …… 只要 **Falcon** 接通电源，它就可以 “强迫所有附近的移动电话和其他蜂窝数据设备连接到它”，并可以帮助政

府当局 “找出任何目标 [隐藏] 的确切住所” …… https://iyouport.substack.com/p/ibm?utm_source=publication-search

攻击者可利用**IMSI**捕获器将人员与手机号码关联起来。例如：

- 在公共示威活动中，记录示威现场所有手机的号码，并通过移动网络运营商的合作后续获取这些号码所对应的用户姓名。
- 作为物理监控行动的一部分，记录目标手机号码或与目标有联系的人员的手机号码。

攻击者还可以使用**IMSI**捕获器记录手机活动。例如：

- 在无需移动网络运营商配合的情况下记录目标手机的活动（在某些情况下这可能需要搜查令）。
- 在攻击者知道手机使用位置但未知其手机号码时，记录目标手机的活动。

📌 对应的镇压战术：指控。

[image]

返回：[image]如何应付政府使用黄貂鱼对公民进行的大规模间谍行为？

返回：[image]泄漏文件显示间谍已经能绕过 Signal 的加密，那么端对端还有用吗？

返回：[image]如何识别抗议活动中可见的和不可见的监视

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

自卫措施

镇压行动案例

[image]

镇压应对措施

为镇压做准备是指采取预防措施，以尽可能将镇压所造成的影响降至最低。镇压只有在我们准备不足的情况下才最危险。

这项准备工作并不是容易的，一直绷紧的防御意识可能导致心力交瘁。但事实证明，这是值得的，它实际上能让我们行动得更自由。

为镇压做准备可以有实际层面，也可以有心理层面。

关于实际层面准备工作的一些例子：

- 确保您的同志 —— 至少是亲密团队中的其他战友 —— 都能知道在您被捕时他们应该做什么，例如您应该按照保密等级提前分享工作电子邮件登录凭据或家门钥匙，安排人照顾孩子或支付您的租金或保释金等等。

- 您需要确保即使您被监禁，您的项目仍然能继续进行，有时这就像提前共享密码一样简单。

- 进行搏击训练，可以让您更好地应对许多监狱中普遍存在的囚犯之间的暴力行为。 在这里看到一些搏击训练建议 [image]街头政治对抗技巧提示（就是打架）

- 如果您所在的地区对毒品赌博这类东西定义为高度刑事犯罪，就请千万绕避这些东西！这不是所谓的洁身自好这么简单，因为镇压者手握定罪权，他们会用这些东西给您👎栽赃 从而施压于您，威胁您去做他们真正想让您做的事 —— 比如去做线人出

卖您的同伴、再比如去做替死鬼以帮助镇压者完成“办案指标”……“小辫子”可能被强行安装。不要给他们这样的机会。

- 还有更多。

关于心理层面准备工作的一些例子：

- 与遭受镇压的同志们交流，谈论他们的经历，包括被监禁的经历。了解和理解。恐惧只出现在未知的情况下。所以消除恐惧的方法就是，让它“已知”。

- 克劳迪奥·拉瓦萨自传中描述过这样的经历，他在山中的一所房子里隐居了一个月，为可能被监禁做准备。 https://www.notrace.how/documentation/claudio-lavazza-seclusion-experience.pdf

以下是一些您可以在亲密团队和您的社区安全培训工作中使用的导图。这只是基本框架，请根据您的本地环境进一步扩展它们。

关于“准备工作”和救助流程

[image] 1、心里有数 [image] 2、做准备。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 3、当亲友被捕时应该怎么办。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 4、如果警察抢走了电子设备。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 5、您需要提起警惕的一些“小”状况。这些情况有可能并不小，请保持防御意识。 [image] 6、如果被捕的是您的同伴，该怎么办。您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

此自卫措施用于应对的镇压手段

[image]
[image]

警方档案(网格)

警方档案是由执法机构保存的纸质或数字记录。警方档案包含涉及方方面面的海量数据，可以无限期或长期保存，并且可以使用数字工具进行高效的分析和交叉引用。

警方档案的典型例子包括：

- 政府颁发的身份证件数据库（身份证、驾驶执照、护照、社保卡等等）。
- 生物识别信息数据库（面部照片、指纹、DNA、步态等等）。
- 身份核查记录、罚款记录、逮捕记录、调查程序记录、司法程序记录、及定罪记录。

□

延伸：https://web.archive.org/web/20210716043727/https://iyouport.substack.com/p/06d

延伸：https://web.archive.org/web/20250306142821/https://iyouport.substack.com/p/faa

延伸：https://web.archive.org/web/20250202144356/https://iyouport.substack.com/p/f83

延伸：https://web.archive.org/web/20250305214504/https://

iyouport.substack.com/p/4d2

https://iyouport.substack.com/p/06d

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]
🌍

跨国维稳

跨国维稳（或者说“国际合作”）指的是不同国家执法和情报机构之间的信息交换/共享。

延伸：https://iyouport.substack.com/p/c20?utm_source=publication-search

延伸：https://iyouport.substack.com/p/protonmail-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/82d?utm_source=publication-search

延伸：https://iyouport.substack.com/p/8f5?utm_source=publication-search

延伸：https://iyouport.substack.com/p/-192-?utm_source=publication-search

国际合作可用于：

- 情报交流。
- 协助跨国界对嫌疑人进行指控、逮捕和驱逐。

- 国际合作可通过非正式渠道进行，也可通过正式组织如国际刑警组织来实施。（附 国际刑警组织通缉人员数据库）

📌 对应的镇压战术：逮捕、指控。

【更新：2026.04.27】

[image]

有一种短信，它针对性发送给你，
但它不会显示在你的手机屏幕上、不会导致手机震动，也没有任何记录，甚至在运营商那里都查不到收发痕迹，
所以你肯定不会知道自己接收过这样的短信
—— 但就是这个短信，把你的手机变成了随身间谍。
……
这件事在全世界发生，主要用于跨国追捕、绑架谋杀，
这一威胁已经存在十年以上，
而如今，它已经实现了产业化、规模化，形成了一个稳固的市场。
……
没有解决方案，只要你随身携带一部开启的智能手机，这一威胁就随时可能发生。

BACK [image] 全球噩梦 - 跨国电信生态系统下的隐形枷锁：公民实验室调查“Bad Connection”

【更新：2026.04.29】

[image]

BACK 🇨🇳中国跨境数字镇压的工业化和私营承包商演变：公民实验室最新报告“Tall Tales”

镇压行动案例

[image]
[image]

恶意女仆和查抄

恶意女仆攻击即物理访问，是指攻击者通过直接接触的方式访问电子设备以获取其数据或破坏设备的过程。

攻击者可以物理访问的电子设备包括：

- 计算机、手机和存储设备（如硬盘、USB 闪存盘、SD 卡）。
- 打印机、相机、“智能”电视。
- 联网车辆。例如，现代车辆中的导航系统可以存储车辆位置记录。延伸：https://iyouport.substack.com/p/c9e?utm_source=publication-search

如果攻击者可以物理访问设备，他们可以：

- 读取设备所有未加密的数据，或其加密数据（如果设备处于开启状态，则其加密功能无效）。
- 通过恶意软件入侵设备。
- 通过硬件键盘记录器入侵设备。

攻击者可通过以下方式物理访问设备：

- 在搜查房屋或秘密入侵房屋时。
- 在您被逮捕且随身携带该设备时。
- 在边境强行检查时。
- 通过有权访问该设备的渗透者或线人。

📌 对应的镇压战术：指控。

自卫措施

[image]

被捕支援

被捕支援是为狱中战友组织物质、后勤和情感支持的关键过程。

这不仅仅是道德义务问题，同等重要的是安全问题 —— 如果人们能感到自己得到了支持，并且能确信这份强大的爱意和力量与他们为之冒着失去自由的风险所从事的解放运动息息相关，他们就不太可能成为告密者。

[image]

返回：[image]充分利用大规模逮捕，以及被捕后怎么办：示威参与者指南S05E07

[image]

返回 - 需要提前做的事情：[image]镇压应对措施

常见的囚犯支持举措包括：

- 写信。寄明信片。表达支持和爱，抹去狱中人的内心孤苦。
- 向囚犯或其亲属提供直接的经济支持。
- 筹钱 - 交保释基金和律师费。
- 继续运行被监禁同志主持的项目或斗争，并以对狱中同志有意义的方式表达团结。

- 越狱协助。

此自卫措施用于应对的镇压手段

[image]
[image]

网络取证

网络取证是指监控和分析网络流量。

网络信息具有易失性，其设计目的是传输后即被丢弃，因此监控网络流量需要采取主动措施。许多国家都有建立网络监控中心，这些中心会存储海量网络信息，保存时间可达数天、数月甚至数年，以便后续分析。

攻击者也可通过与您的互联网服务提供商合作、利用恶意软件入侵您的家庭路由器，或从停留在您家外面的监控车辆里通过监控您的有线或无线网络连接来监控您的网络流量。

[image]

返回：

[image]

返回：[image]如何检查您的VPN连接是否实际加密

由于大多数网站、电子邮件提供商和即时通讯应用程序使用SSL/TLS加密（即“https”中的“s”），监控您网络流量的攻击者通常知道您访问了哪些网站，但不知道您在这些网站上做了什么。如果您使用Tor，监视您网络流量的对手知道您使用Tor，但不知道您访问了哪些网站或在这些网站上做了什么。

[image]

返回：[image]使用Tor保护自己时千万不要做这9件事

Tor易受关联攻击，但此类攻击即使对强大对手而言也不容易实施。关联攻击的成功案例之一是对无政府主义黑客杰里米·哈蒙德的起诉：通过网络流量分析获得的他在聊天室中使用的化名身份“在线”的时间，与物理监视行动观察到他在家中的时间相关联，以证明该化名身份属于他。□ 案件详情：https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

假身份

假身份是全套的，用来取代您的既定身份。可以拥有多个假身份证，并且可以根据具体情况在既定身份和不同假身份证之间进行切换。

假身份可能包括：

- 假的姓名、出生地点和日期以及其他个人信息。
- 假的家庭历史、工作历史和其他背景信息。
- 伪造的身份证件。

可能需要使用假身份的情况包括：

- 为了减轻网络映射 导致的连锅端逮捕，或避免在强行身份检查 中暴露 。
- 在寻找和装备[image]藏匿点或安全屋 的过程中 。
- 在不得不跑路[image]隐姓埋名 的情况下。

此自卫措施用于应对的镇压手段

[image]
[image]

服务提供商协助调查

向您提供服务的公司 —— 即 那些监视资本家 —— 因此掌握了关于您的非常多的私密信息。如果他们出于任何动机（不论是经济的还是政治的）选择与您的对手合作来对付您，是非常危险的事。某些情况下比线人更危险。

[image]

返回：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

不幸的是，很多时候，国家甚至可以立法强制服务提供商交出任何信息。以防疫为借口的大规模监视深化和合法化，应该再一次提高人们的警惕。

□

延伸：https://iyouport.substack.com/p/lr-covid-1984-?utm_source=publication-search

政治环境和外交关系在此也有影响。比如：

- 西班牙是一个对其管辖范围内的公司拥有高度控制权的国家，可以非常容易地迫使本地移动网络运营商提供任何用户的信息。

- 伊朗是一个与加拿大没有外交关系的国家，不能强迫加拿大税务局提供加拿大纳税人的信息。

同时要知道，非国家对手和国家都可以通过以下方式获取服务提供商的信息：

- 腐败：收买腐败分子（如服务提供商公司的雇员、警察）出售的服务提供商信息。贪婪是无法避免的；并且，公司也更倾向于让个别员工来背负全责。
- 数据泄露：例如服务提供商的数据库被黑客入侵，对手在黑市上购买。数据保存得越多，其价值就越大，就越吸引攻击者。泄漏无法避免。所以日常的数字卫生和最小化原则，是很重要的。

[image]

返回：[image]即使数据是匿名的，您的身份仍然可以被识别

[image]

返回：[image]大保健应该成为习惯：变得难以被追踪的简单方法 S03E06

📌 对应的镇压战术：指控。

2个子项目

[image]

匿名着装

匿名着装是指选择服装时兼顾两个目标：隐藏身体特征，及，确保服装本身无法用于识别身份。

隐藏身体特征

为隐藏身体特征，可采取以下措施：

- 遮盖面部：佩戴能完全覆盖面部（包括眉毛至鼻梁上部）的面罩。
- 隐藏身体其他部位：穿着长袖上衣、戴手套、长裤或无特征的高筒袜。
- 隐藏肤色：确保无皮肤暴露，包括眼周、衣袖与手套间的接缝处、裤脚与袜口之间。
- 隐藏体型与步态：穿着宽松的衣物，比如肥大的长袍。但需注意不能过于显眼，且不能妨碍跑跳等快速运动。（更多可参见 [image]生物特征隐藏，其中包括掩盖步态特征的建议）。

确保服装无法用于识别身份

为确保行动期间穿着的服装无法用于识别身份，可遵循以下规程：

1、 BACK 匿名购置两套专用于行动的服装，即区分“便服”与“行动用服饰”：

- 便服指的是日常公共场合穿着的普通服装。可包含隐藏身体特征的物品（如帽子、“防疫”口罩），但需避免引起怀疑。
- 行动服饰需充分隐藏身体特征，具体要求参见上述。

2、远离行动地点后，在确认没有监控摄像头或“目击者”的合适场所更换到便装。

3、接近行动地点时，在合适场所换上行动服。

4、执行行动。

5、撤离过程中，在合适的地方换回便服。

6、远离行动地点后，在合适场所换回日常服装。

7、安全处置便服与行动服。

“黑群”战术

黑群战术是一种特定的匿名着装形式，示威者群体通过统一穿着（通常为全黑色）使监视者难以辨识其中的具体个人，形成视觉同质化。

关于黑群策略的方法、利弊分析、注意事项，详见下述：

[image]

返回：[image]如何启动黑群 - 从准备到行动：街头实战指南 S05E16

此自卫措施用于应对的镇压手段

[image]
[image]

警察巡逻

是指在特定区域内巡逻以进行监视和维稳的执法行为。警察巡逻可以作为例行行动，也可以作为对特定区域内潜在威胁的回应。

> 南华早报：这项研究由中国政府资助，旨在评估全国范围内对警用机器人的需求。研究发现，一台标准机器人每天可以巡逻80公里（50英里）的街道，并检查200多名“可疑人员”，这相当于中国男女警察平均工作量的10倍以上。 https://www.scmp.com/news/china/science/article/3200526/chinese-robocop-can-boost-police-patrol-resources-10-fold-survey-finds

□

延伸：https://web.archive.org/web/20250202155312/https://iyouport.substack.com/p/ai-

[image]

交通工具

警察巡逻可以使用不同的交通工具，比如：

- 有标记的或没有标记的车辆。
- 徒步巡逻。

- 直升机、无人机和侦察机。

常规巡逻

常规警察巡逻通常在警察局周围的广阔区域进行。其目的是建立可见的警察存在，以威慑潜在犯罪分子，偶尔也能当场抓到一些人。

针对特定状况的巡逻

如果警方获悉某一区域存在值得调查的“威胁”——比如抗议活动、起义、直接行动，他们将派出一队或多队巡逻队。从警方获悉“威胁事件”、到巡逻队抵达的时间，取决于待巡视区域与最近的可用警力单位之间的距离。

警方可通过以下方式获悉所谓的“威胁”情报：

- 例行巡逻偶然发现。
- 守卫或平民的举报。
- 报警系统（例如建筑物内的运动探测器），无论是直接监测还是通过监控报警系统的安保公司。
- 警察监控实时闭路电视摄像机的画面。
- 线人或告密者。

[image]

返回：[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image]
[image]

隐蔽性地突袭住所

这里特指秘密突袭，在住户不在场的情况下对住宅进行秘密搜查。

对手可以通过秘密的破门而入，以：

- 搜查/收集信息。
- 在住宅内安装隐蔽的监控设备。
- 在数字设备上安装恶意软件。

通常，对手不希望住户知道秘密入室行为的存在。如果相反则不属于“秘密”入室（比如具有恐吓性质的入室行动）。

因此，通常情况下：

- 如果住宅的门是锁着的，对手必须在不明显破坏门的情况下进入室内。他们可以通过撬锁/万能钥匙、或者向建筑物所有者索要钥匙以进入，再或者从窗户、烟囱中进入。
- 对手会避免拿走物品或移动物品，避免留下入室的证据。

除了进入室内，对手还可以拿走住宅外的垃圾，以期找到有价值的信息（例如书面笔记、法医证据如DNA痕迹等），即垃圾箱潜水。

返回：[image]心里有数：如果您已成为目标：来自内部和外部的威胁和抵御

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

监控侦测

监控侦测是指侦测您是否受到[image]物理监控（上岗） 的措施（即检测您是否被对手直接观察）。

监控侦测分为两种：被动的和主动的。 [image]反监视 是主动侦测的一种复杂形式。

被动监控侦测

是指在不偏离正常行为程序的情况下检测到监视的情况。示例包括：

- 在行驶的车辆中不断检查后视镜和侧视镜，以检查是否有跟踪您的监视车辆。
- 随时悉心聆听周围的声音，以留意头顶上是否有飞过无人机或直升机。
- 以及更多。

主动监控侦测

是指通过采取超出日常行为范围的行动来检测监视的存在，目的是迫使潜在的监视行动暴露自身。

示例包括：

- 在两点之间行驶时选择不合理的路线，例如明显的绕路。如果某些/某个行人或车辆也立刻选择了与您相同的不合理路线，则他们可能是监控人员。如果可能，您应该提供采取这种不合理路线的正当理由（例如在沿途的商店停留），以便监控人员无法察觉您正在进行监控侦测。

- 驾驶过程中意外掉头。如果您被一支不怎么专业的监控小组（或仅一辆监控车）跟踪，监控车可能会模仿您的掉头动作，这就暴露了他们正在跟踪您的事实。但如果您被一支很专业的多车监控小组跟踪，监控车不会模仿您的掉头动作，因为这会引起怀疑。不过您的意外掉头仍然会引起他们的异常反应，这有助于您发现他们。如果可能的话，您应该提供掉头的合理理由，以便监控人员无法察觉您正在进行监控侦测。 比如买路边的东西等等。

反监视

[image]反监视 是指在可信第三方（例如一人或多人）的帮助下，侦测到监视行为。

以下是一个反监视行动的示例：

1、选择一条您在反监视行动中要走的路线。这条路线对于潜在的监视行动来说应该合乎逻辑，但对于其他人来说则不合逻辑（这样可以将可能的误解率降至最低，同时也不至于让监视方觉察到）。并且这条路的沿途应该包含几个“侦测点”，以便第三方能够尝试侦测监视行动。

例如，您可以从家出发，在您所在城市的三四家五金店停留，假装对某件商品进行比价，然后返回家中。这条路线对于潜在的监视行动来说似乎是合乎逻辑的，但其他人不太可能会走同样的路线，更不用说按照与您相同的顺序在相同的商店停留了。

2、当您沿着选定的路线行驶时，第三方会确保他们先于您到达每一“侦测点”，但不会与您走相同的路线（这样他们就不会被潜在的监控行动发现）。为了实现这一点，第三方可以使用比您更快的出行方式，或者在您之前从每一侦测点抢先出发，或者使用多个协作小组。

3、在每个侦测点，第三方都会记录在您之后到达的行人和车辆。如果第三方注意到同一行人或车辆出现在两个或多个侦测点，则意味着他们可能参与了监控行动。第三方还可以侦测到监控人员的典型行为，例如通过隐藏在身上的无线电发送信息、通过视觉信号相互交流、意外奔跑等。

其他注意事项

如果对手注意到您正在进行监视侦测，他们可能会做出调整，变得更加谨慎。因此，在进行监视侦测时，应尽可能避免暴露自己的意图。即使成功侦测到监视，也应避免打草惊蛇。

[image]

返回：[image]在你的日常生活中应用隐蔽野战技术 - 简单方法抵御敌对监视: 反侦基础课 S06E06C

返回：[image]用“眼”识人 - 你想知道自己在一个“间谍”的眼中是什么样吗: 反侦基础课 S06E06A

推荐资料

- Surveillance Countermeasures（这是暗网链接）

此自卫措施用于应对的镇压手段

[image]
[image]

语言指纹

法医语言学是将语言学知识应用于识别文本作者或声音背后的人。作者识别（也称为文体测量学）基于对语言使用某些模式的分析：词汇、搭配、拼写、语法等。声音识别基于语音（语音学）和声音的声学特性。

作者识别

作者识别可用于确定：

- 谁撰写了发布在互联网上的匿名行动声明、谁透露给报纸的机密消息。
- 多个匿名行动声明是否可能由同一人或同一群体撰写。
- 谁撰写了在房屋搜查、秘密突袭或逮捕过程中发现的描述“非法活动”的计划。

语音识别

语音识别可用于确定：

- 谁在使用被监听的手机通话，或者隐藏窃听器的录音中说话的人是谁。

- 谁在打给政府机构的电话中进行炸弹威胁。

推荐书目

1、《Counteracting Forensic Linguistics》
2、《Who wrote that? (Wer schreibt denn da?)》

📌 对应的镇压战术：指控。

🚫

如果您曾经在社交媒体或网站上公开发表过不少可追踪到您真实身份的文章/帖子，并且您担心自己不擅长掩盖语言指纹，那就请不要亲自撰写最重要的行动声明和动员令。您的团队（合作者）中应该有人擅长掩盖语言指纹，此人可作为编辑的角色在幕后合作，并且应该擅长 数字最佳实践 。

[image]

返回：[image]袜子木偶 - 分身创建的小技巧

更新 [V1.1.2.20260324]

现在，LLM可以在各个平台上对你的写作风格进行指纹扫描。这是一篇近期比较惹火的论文。该论文显示，通过使用语义嵌入 + 推理层，可实现90% 的精确率下达到 68% 的召回率。

您以为的“匿名”帐户和您的 LinkedIn 已不再是两个独立帐户，它们现在只是模型中的两个节点。

换句话说，如果数字世界里存在关于您的近乎**LinkedIn**个人资料一般的真实身份信息，想要通过分身实现匿名已经非常困难。而且可能会越来越困难。

社交媒体情报从来不是新鲜事。书写习惯、措辞风格、语态节奏、标点符号、感兴趣的话题、关注者圈子，等等所有这一切，现在都在被更快速地结合在一起，形成了一个大多数人都极难保护的身份指纹。这不是现在开始的，从大数据政变实现的那年就已经开始了。只是在**AI**的助力下，这场噩梦正在以百万倍的速度膨胀。

简单说：您越倾向于展示自己，就越危险。

[image]

这场噩梦的开端是大数据经济的崛起：[image]单向镜的背后：监视资本家和政府的联手一直在如何折腾你？

基本原理：[image]即使数据是匿名的，您的身份仍然可以被识别

该论文采取的只是一种很朴素的方法论，这种方法对那些习惯于在帖子中透露大量职业或个人生活细节的自恋型/自我表达型的数字用户最为有效。但真正令人担忧的是其跨平台方面的能力，和其毫无疑问会快速增长的功能性 —— 别忘了对此等能力最感兴趣的不会有什么好人，而且大多是权势阶层，国家暴力机器，他们有充分动机对该能力进行大举投资。这至少意味着你我的防御成本和压力都在快速攀升。

在下面看到该论文。

[image]

https://arxiv.org/abs/2602.16800

那么分身还有用吗？

绝对有用，而且正变得前所未有地重要和必要；尤其是，需要加倍努力和小心才能降低风险。

提示：

- BACK [image]数字技术限制和最佳实践 对激进社群至关重要！请尽快纳入入门培训。强调关注前提：数字技术限制 —— 练习并习惯于非必要不采取的原则（只要能见面，就不必在网络上交流；只要能在纸上做，就无需应用程序...）。切勿完全信赖任何你没有控制权的设施。

- 类似 BACK [image]户外无设备对话 措施非常值得扩展适用范围。这意味着帮助更多战友习惯于这一方法， 将隐私素养纳入价值观共识。

- 在自己的团队中警惕安全性虚无主义论调！针对数字风险焦虑，组织者应学习针对性提问，邀请对方具体的、详细地描述每一种担忧和需求，并一起寻找解决方案。而不是放任悲观情绪弥漫削弱决策理性。

- 主流应用和平台非不得已均可减少使用。逐渐适应开源自由软件替代品 BACK [image]隐私自助：流行产品的开源替代品目录 。可在这里查看并分析自己的风险环境，以做出最适合的决策： BACK [image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式 ； BACK [image]社交媒体上的行动主义安全性:框架手册

- 帮助您所在的社群和队友学习数字世界的底层逻辑，并训练自检自卫的意识。培训可从这里进入： BACK 🔍开源情报 ； BACK [image]技术是愚蠢的-这就是为什么您应该格外小心：基本手册给行动者、敏感人士和任何期待安全的普通公民

- 团结人类！真正的人类！当您在街头迎战催泪瓦斯和橡皮子弹时，只有血肉之躯能助一臂之力。 安全的基础设施是长期稳定的正向亲密关系 ，除此外的其他一切都是临时采取的工具。

[image] BACK [image]当科技巨头走向战争...

自卫措施

镇压行动案例

[image]
[image]

警察巡逻

是指在特定区域内巡逻以进行监视和维稳的执法行为。警察巡逻可以作为例行行动，也可以作为对特定区域内潜在威胁的回应。

> 南华早报：这项研究由中国政府资助，旨在评估全国范围内对警用机器人的需求。研究发现，一台标准机器人每天可以巡逻80公里（50英里）的街道，并检查200多名“可疑人员”，这相当于中国男女警察平均工作量的10倍以上。 https://www.scmp.com/news/china/science/article/3200526/chinese-robocop-can-boost-police-patrol-resources-10-fold-survey-finds

延伸：https://web.archive.org/web/20250202155312/https://iyouport.substack.com/p/ai-

https://iyouport.substack.com/p/ai-

交通工具

警察巡逻可以使用不同的交通工具，比如：

- 有标记的或没有标记的车辆。
- 徒步巡逻。

- 直升机、无人机和侦察机。

常规巡逻

常规警察巡逻通常在警察局周围的广阔区域进行。其目的是建立可见的警察存在，以威慑潜在犯罪分子，偶尔也能当场抓到一些人。

针对特定状况的巡逻

如果警方获悉某一区域存在值得调查的“威胁”——比如抗议活动、起义、直接行动，他们将派出一队或多队巡逻队。从警方获悉“威胁事件”、到巡逻队抵达的时间，取决于待巡视区域与最近的可用警力单位之间的距离。

警方可通过以下方式获悉所谓的“威胁”情报：

- 例行巡逻偶然发现。

- 守卫或平民的举报。

- 报警系统（例如建筑物内的运动探测器），无论是直接监测还是通过监控报警系统的安保公司。

- 警察监控实时闭路电视摄像机的画面。

- 线人或告密者。

[image]

返回：[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image]
👀

大规模监视

大规模监控是指对整个社会或相当一部分人口进行的普遍监控。大规模监视是政权进行社会控制的基线。

□

延伸：https://web.archive.org/web/20220125223716/https://www.iyouport.org/%E6%B3%84%E6%BC%8F%E6%96%87%E4%BB%B6%E8%AF%81%E5%AE%9E%EF%BC%9A%E6%9C%89%E6%9B%B4%E5%A4%9A%E7%9A%84%E7%BE%8E%E5%9B%BD%E7%A7%91%E6%8A%80%E5%B7%A8%E5%A4%B4%E6%94%AF%E6%8F%B4%E4%B8%AD%E5%9B%BD%E5%BA%9E/

延伸：https://web.archive.org/web/20220123211404/https://www.iyouport.org/%E7%BE%8E%E5%9B%BD%E7%A7%91%E6%8A%80%E5%B7%A8%E5%A4%B4%E5%A6%82%E4%BD%95%E5%B8%AE%E5%8A%A9%E4%B8%AD%E5%9B%BD%E5%BB%BA%E7%AB%8B%E5%A4%A7%E8%A7%84%E6%A8%A1%E7%9B%91%E8%A7%86%E7%B3%BB%E7%BB%9F/

📌 对应的镇压战术：威慑、指控。

大规模监控的4个子项目

[image]
[image]

警察巡逻

是指在特定区域内巡逻以进行监视和维稳的执法行为。警察巡逻可以作为例行行动，也可以作为对特定区域内潜在威胁的回应。

> 南华早报：这项研究由中国政府资助，旨在评估全国范围内对警用机器人的需求。研究发现，一台标准机器人每天可以巡逻80公里（50英里）的街道，并检查200多名“可疑人员”，这相当于中国男女警察平均工作量的10倍以上。 https://www.scmp.com/news/china/science/article/3200526/chinese-robocop-can-boost-police-patrol-resources-10-fold-survey-finds

□

延伸：https://web.archive.org/web/20250202155312/https://iyouport.substack.com/p/ai-

https://iyouport.substack.com/p/ai-

交通工具

警察巡逻可以使用不同的交通工具，比如：

- 有标记的或没有标记的车辆。
- 徒步巡逻。

- 直升机、无人机和侦察机。

常规巡逻

常规警察巡逻通常在警察局周围的广阔区域进行。其目的是建立可见的警察存在，以威慑潜在犯罪分子，偶尔也能当场抓到一些人。

针对特定状况的巡逻

如果警方获悉某一区域存在值得调查的“威胁”——比如抗议活动、起义、直接行动，他们将派出一队或多队巡逻队。从警方获悉“威胁事件”、到巡逻队抵达的时间，取决于待巡视区域与最近的可用警力单位之间的距离。

警方可通过以下方式获悉所谓的“威胁”情报：

- 例行巡逻偶然发现。
- 守卫或平民的举报。
- 报警系统（例如建筑物内的运动探测器），无论是直接监测还是通过监控报警系统的安保公司。
- 警察监控实时闭路电视摄像机的画面。
- 线人或告密者。

[image]

返回：[image]了解诱捕战略：如果政府间谍要求你做线人怎么办？如何判断一个人是否可能是线人？

[image]
🚔

增加警力

增加警力是指警察在特定时间和地点调动更多警力的过程，其原因有二：要么是为了威慑，要么是镇压战术的调整（接下来会有大动作的那种）。

增加警力的例子包括：

- 特定区域的警察巡逻更加频繁。
- 在公众示威活动现场部署更多的警力和车辆。在示威活动开始前的几个小时里，警力和车辆可能会聚集在示威活动周围或预期目标周围的街道上。这种聚集为警方在示威活动之前、期间和之后进行公开监视提供了机会。

📌 对应的镇压战术：逮捕、威慑。

自卫措施

[image]
[image]

物理监控（上岗）

物理监视是指为了收集信息/情报而对目标人员或活动进行直接的观察。物理监视行动通常由一个或多个监视小组执行，这些监视小组由经过特殊训练的人员组成，称为监视操作员。

由于物理监视需要在实地部署监视操作员，有时需要持续较长时间，因此它通常是一种资源密集型和人员密集型的监视方法。也是一种消耗维稳经费的做法。中国大陆朋友熟悉的“上岗”，就是这类做法中相对简单且常见的一种。

3个子项目

[image]

计算机和移动设备取证

计算机和移动设备取证是一门技术性极强的学科，这里所说的不是指警察查手机那种（尽管技术原理上大同小异），而是旨在识别电子设备上的入侵行为的调查技术。

[image]

返回：[image]设备好像被黑了怎么办？ - 数字急救包

[image]

返回 - 工具：[image]检查智能手机是否感染了病毒

如果您怀疑您的某个设备被入侵了，并且想要了解有关疑似入侵的更多信息，您可以向非营利组织如 AccessNow 或国际特赦组织寻求帮助。但需要注意的是，它们都是合法组织，如果国家提出要求，它们需要依法合作。

对于无政府主义者和其他激进反叛行动者来说，非常建议您在自己的亲密团队或同道社区中包含类似高技术的互助服务。如果您对此有想法，或者有红队经验和能力，欢迎联系我们。

此自卫措施用于应对的镇压手段

[image]
👀

大规模监视

大规模监控是指对整个社会或相当一部分人口进行的普遍监控。大规模监视是政权进行社会控制的基线。

延伸：https://web.archive.org/web/20220125223716/https://www.iyouport.org/%E6%B3%84%E6%BC%8F%E6%96%87%E4%BB%B6%E8%AF%81%E5%AE%9E%EF%BC%9A%E6%9C%89%E6%9B%B4%E5%A4%9A%E7%9A%84%E7%BE%8E%E5%9B%BD%E7%A7%91%E6%8A%80%E5%B7%A8%E5%A4%B4%E6%94%AF%E6%8F%B4%E4%B8%AD%E5%9B%BD%E5%BA%9E/

延伸：https://web.archive.org/web/20220123211404/https://www.iyouport.org/%E7%BE%8E%E5%9B%BD%E7%A7%91%E6%8A%80%E5%B7%A8%E5%A4%B4%E5%A6%82%E4%BD%95%E5%B8%AE%E5%8A%A9%E4%B8%AD%E5%9B%BD%E5%BB%BA%E7%AB%8B%E5%A4%A7%E8%A7%84%E6%A8%A1%E7%9B%91%E8%A7%86%E7%B3%BB%E7%BB%9F/

📌 对应的镇压战术：威慑、指控。

大规模监控的4个子项目

周密的行动计划

计划不仅要细致，还要多手准备，而且要合理。这需要在执行[image]地形侦查 的基础上制定。

周密的行动计划必须明确参与行动的每个人的角色以及他们的任务与其他人的任务之间的关系。

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

[image]

返回：[image]充分的准备和应急反应同样重要：整体安全S01E07 - 计划是 “活的”

例如：考虑到对手的预期反应时间，往返行动地点的最佳路线是什么？您会在行动地点停留多长时间？或者，您的撤离路线沿途有哪些地方可能会干扰追击（例如，对手是否需要下车步行跟踪）？制定行动计划是一种威胁建模 —— 哪些地方可能出错？您将采取哪些缓解措施？以及如何实施？例如，您将如何在进入行动汇合点之前进行[image]反监视 ？

此自卫措施用于应对的镇压手段

[image]
[image]

视频监控

大规模视频监控（即大规模CCTV监控网络）是指对来自视频监控摄像头的视频和音频数据进行大规模收集、存储和分析。旨在捕捉经过某个空间的所有人员身份，并将其覆盖范围扩大到尽可能广阔的区域。

如今一些国家的监控摄像头数量甚至超过了人口数量。

□

延伸：https://iyouport.substack.com/p/lr--a15

延伸：https://web.archive.org/web/20201027144114/https://www.iyouport.org/%E4%B8%AD%E5%9B%BD%E5%90%9160%E5%A4%9A%E4%B8%AA%E5%9B%BD%E5%AE%B6%E5%87%BA%E5%8F%A3ai%E7%9B%91%E6%8E%A7%E6%8A%80%E6%9C%AF/

https://iyouport.substack.com/p/lr--a15?utm_source=publication-search
https://web.archive.org/web/20201027144114/https://www.iyouport.org/%E4%B8%AD%E5%9B%BD%E5%90%9160%E5%A4%9A%E4%B8%AA%E5%9B%BD%E5%AE%B6%E5%87%BA%E5%8F%A3ai%E7%9B%91%E6%8E%A7%E6%8A%80%E6%9C%AF/

数据采集

CCTV视频数据的来源包括：

- 街道或其他公共场所的监视摄像头。
- 私人建筑物内的监视摄像头（如商店、办公室等）。
- 公共交通工具上的摄像头（如公交车、火车、高速公路等）。
- 家庭监控系统，如亚马逊Ring等等。□ 延伸：https://iyouport.substack.com/p/e6d?utm_source=publication-search
- 车载监控系统，如特斯拉汽车上的系统。□ 延伸：https://iyouport.substack.com/p/d21?utm_source=publication-search

CCTV摄像头的质量、范围、夜视能力、是否配备麦克风等特性差异显著。

存储

采集后的监控录像通常会存储一段时间（从数天到无限期不等）。

□

延伸：https://iyouport.substack.com/p/a19?utm_source=publication-search

分析

监视者可以分析监控录像：

- 若摄像头集成到中央网络，可进行实时分析。实时分析可作为

常规监控的一部分，或在特殊事件（如示威活动）期间进行。

- 若监控录像已被存储，可进行事后分析。事后分析可通过面部、步态、声音等特征识别目标人。

□

延伸：https://iyouport.substack.com/p/-192-?utm_source=publication-search

延伸：https://iyouport.substack.com/p/f38?utm_source=publication-search

CCTV录像的分析可通过以下方式进行：

- 人工分析。

- 自动化系统分析，如自动车牌识别系统或人脸识别系统。

□

延伸：https://iyouport.substack.com/p/lr--bc3?utm_source=publication-search

□

延伸：https://iyouport.substack.com/p/c9e?utm_source=publication-search

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]
[image]

法医取证

法医学是将科学应用于调查，以收集、保存和分析证据。其研究领域广泛，包括：DNA分析、指纹分析、血迹形态分析、枪械检验和弹道分析、工具痕迹鉴定、血清学检测、毒理学、毛发和纤维分析、鞋类和轮胎胎面分析、药物化学、油漆和玻璃分析、语言学、数字音频、视频和照片分析等等。

除了将嫌疑人的身份与特定行为相关联外，法医学还常用于将个别行为相互关联。

法医学家经常出现在庭审中作为“专家证人”作证。

📌 对应的镇压战术：指控。

10个子项目

[image]

数字技术限制和最佳实践

数字技术限制和最佳实践意味着限制科技对您的生活的触角。尽量限制您对数字设备的使用，尤其是在进行敏感活动时。也就是说，在使用数字设备时，您可以遵循以下最佳实践。

不要使用手机，或将手机留在家中

手机位置随时会被追踪，沿途所有基站都会暴露您，并且还容易被黑客入侵。如果可能的话，请勿使用手机。

如果必须使用手机：

- 使用 GrapheneOS 、安装端到端加密消息应用程序。请勿使用传统的短信和电话。
-

[image]

返回：📱警察如何利用抗议者的手机追踪每个人

返回：[image]警察查手机的东西长什么样？—— 从技术角度看移动设备取证

返回：[image]数字取证正在泛滥：政府可以从你的手机中提取哪些数据？

返回：[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

使用面向安全的操作系统

- Debian 或 Qubes OS 用于日常电脑使用。
- Tails 用于敏感计算机的使用，例如阅读敏感文章、为某项行动进行研究、撰写和发送行动声明以及管理敏感网站。
- GrapheneOS 用于手机。

以及，使用全盘加密，和加密卷。

[image]

返回：[image]来自人身的威胁：如何在敌对环境中保护自己 S02E01

使用强密码

您的大多数密码（例如，您用于登录网站的密码）应该由密码管理器生成，并存储在其中（ [image]什么是凭据填充攻击？如何选择密码管理器？ ）。密码可以很长且随机，例如 40 个随机字符。

主密码必须牢记。推荐使用 Diceware 5至10个单词的密码。 您可以使用 KeePassXC（生成密码时选择“密码短语”）或物理骰子生成此类密码。 您应该为每个加密设备使用不同的密码，但对密码管理器数据库可以使用相同的密码（这样您需要记住的密码就更少）。

例如，如果您有一台加密的笔记本电脑、一个 Tails U盘和一部加密的手机，仅此您就需要记住 4 个 5 ～10 个单词的密码（每个设备一

个，密码管理器数据库一个）。这已经不少了。为了确保您不会忘记所有这些密码，您可以：

- 使用记忆技巧，您知道怎么做最合适自己。
- 将密码副本存储在一个U盘上，放在家外一个隐蔽的地方，并用10个单词的Diceware密码加密。您不需要记住这10个单词的密码，而是将其存储在一两位值得信赖的、也遵循这些数字最佳实践的伙伴的密码管理器数据库中。这样，如果您忘记了密码，可以向这些值得信赖的伙伴索要这10个单词的密码，然后取回U盘：在U盘上就能找到忘记的密码。
- 将密码副本存储在一个U盘上，放在家外一个隐蔽的地方，并用20个单词的Diceware密码加密。您不需要记住这个20个单词的密码，而是把它分成两半，每半10个单词，分别写在一张纸上，并将每张纸放在不同的隐蔽处（不要和U盘放在一起）。这样，如果您忘记了密码，可以取出这两张纸，重新构建20个单词的密码，然后取出U盘：在U盘上就能找到忘记的密码。

使用 Tor 或 VPN

使用 Tor 或使用信誉良好的虚拟专用网络 (VPN) 进行互联网活动。

如果您使用 Tor 或 VPN，并且对手正在监控您的网络流量，他们就更难获取有关您互联网活动的数据，例如您访问过的网站、或您在这些网站上进行的操作（他们也更难向您投放恶意软件 ）。

[image]

返回：[image]使用Tor保护自己时千万不要做这9件事

返回：[image]某个VPN可能不可靠的5个标志：如果您不理解技术的话

返回：[image]如何检查您的VPN连接是否实际加密

您应该使用 Tor 进行所有敏感的互联网活动，并尽可能多地进行不敏感的互联网活动。

如果您无法使用 Tor 进行某些非敏感的互联网活动（例如，因为您需要使用阻止Tor的网站），则可以使用 VPN。

如果没有 Tor 也没有 VPN，您就不应该进行任何互联网活动。

使用端到端加密消息应用程序

使用端到端加密消息应用程序进行所有数字通信：

理想情况下，使用端对端且抗元数据的应用程序，例如 Cwtch 或 Briar。 否则，至少使用抗元数据的应用程序，例如 SimpleX 或 Signal。

[image]

返回：[image]如何才能安全地使用端对端加密（比如Signal）：准则

返回 - 工具：[image]一系列安全的即时通信软件和服务

[image]

在本站“工具”专题中搜索“IMs”以找到可能合适您的安全解决方案。

电子邮件不具备元数据防护功能，应尽量避免使用。如果必须使用电子邮件，请使用 PGP 加密，并在可信赖的服务提供商处注册地址。

需要注意的：

Delta Chat 或 Matrix 的元数据抵抗能力不够强。

Telegram 则是选择性的加密。

[image]

返回：[image]Telegram的隐私保护指南，和信息搜索工具

备份您的数据

定期备份您的数据，尤其是您不想丢失的数据，例如密码管理器数据库。使全盘加密功能 加密您的备份。通常的做法是进行两次备份：

- 您在家中保存并经常更新（例如每周一次）的“现场”备份。
- 您保存在家外的“异地”备份，更新频率较低，例如每月一次。

现场备份的优势在于，它拥有您数据的最新版本。异地备份的优势在于，即使您的住所遭到抢劫，条子们也搜不到值得抢走的东西。

以防篡改的方式收纳您的设备

如果攻击者物理访问了您的某个数字设备（比如被查手机了、被强行没收了、被 抄家 ），他们有可能会对您的设备进行篡改 —— 给里面加点东西，以便更直接地持续监视您。为了检测攻击者何时物理访问了设备，您可以使用 [image]防篡改准备 。

[image]

返回：[image]如果您的手机被盗或被警察抢走…

返回：[image]如何保持 Android 设备免受警察的侵害

返回：[image]如何通过一些设置预防iPhone被盗或被警方查抄所造成的损失？

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

匿名购买设备

[image]匿名购买 数字设备有两个好处：

- 如果您的某个数字设备被镇压者获取，他们可能会使用[image]数字取证 从该设备中恢复信息。如果您是匿名购买的，对手可能无法将该设备以及他们恢复的信息与您联系起来。

- 如果您购买数字设备的方式不能让您立即访问该设备（例如，如果您在线订购笔记本电脑），则匿名购买可以防止针对您的对手在您获得访问权限之前篡改该设备（例如，在购买和交付笔记本电脑之间）。这种情况不常见但的确有过案例。总之，只要镇压当局认为足够必要，他们就可以调用足够多的资源来瞄准您。

在不得已的情况下物理销毁您的存储设备

如果要确保攻击者永远无法访问存储设备（例如笔记本电脑硬盘、U盘、SD卡）上的数据，唯一的解决方案就是物理销毁存储设备。

要物理销毁存储设备：

- 首先，重新格式化并覆盖整个存储设备作为额外的安全预防措施。
- 然后，使用高品质家用搅拌机或角磨机将其切碎，理想情况下尺寸小于两毫米。

其他最佳实践

网络钓鱼是社交工程中最常见的攻击方式，攻击者诱骗您泄露敏感信息、或诱导您的误操作以便在您的某个数字设备上安装恶意软件 。

为了避免这种情况，请勿打开不信任的人发送的文件、不要点击陌生人发来的链接，不管他们声称什么理由 —— 谨记“零信任始终验证”原则。

[image]

在本站“心理安全”专题中找到防御社交工程攻击的建议。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。 [image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

此外doxxing又称人肉搜索，一定程度上在中国被称为“开盒”（尽管有部分目的性差异），是指对手在未经您同意的情况下搜罗挖掘并发布您的个人信息，以恐吓您的行为。参与以下防御方法。

[image]

返回：[image]如何知道有人正在线人肉你？6个简单的方法

返回：[image]给活动家的反人肉指南

[image]

生物特征隐藏

生物特征隐藏包括掩盖可用于识别目的的所有生物特征标识（独特的物理或生物特征）的做法。

延伸：https://start.me/w/xLRgMn

此自卫措施用于应对的镇压手段

[image]
□

网络映射

网络映射是对手通过分析特定群体的组织结构和社交关系来获取情报的过程。通过获取这些情报，对手可以筛选出需要进一步调查、逮捕、或可招募为线人的个人。

大数据时代，做到这点真的太容易了 —— 您“随手”刷到的都是您的“朋友”浏览过的小视频；网购站点上会显示支付站点中与您有过支付关系的人的消费习惯；联网汽车勾勒出您的现实生活轨迹 ……

国家机构经常利用社交媒体好友列表（所谓社交媒体情报）进行网络映射，因为此类操作无需搜查令或法律授权。

[image]

返回：[image]社交媒体上的行动主义安全性:框架手册

返回：[image]您在什么时候需要假名、匿名和公开在线身份？– 在线创建和管理身份的思考方式

返回：[image]如何跨社交媒体平台追踪目标人：对抗性思考方式

[image]

返回本站《 操作安全性 》专题，以获取更多防御知识和建议。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

敲门

对手直接来到您的住所并敲门，目的是为了威吓您，和/或获取信息。

敲门行动旨在通过威吓或制造忐忑的心理环境，以识别/引诱有可能透露信息的人，并可能将其招募为线人，同时从嘴巴不严的人那里 收集信息 。

并且敲门不是全部。接下来对手会记录您与敲门者通话或会面后立即联系的人是谁 —— 很大程度上那就是您最信任的人，甚至托付之人，从而可以绘制出你们的关键社交关系网络。

在许多国家，警察直接敲门比进行房屋搜查更容易，因为敲门不需要搜查令或法律授权。

📌 对应的镇压战术：威慑、指控。

自卫措施

特别注意事项

华语朋友都知道“查水表”是什么意思。欺骗性敲门是最常见的逮捕方式，警方可能声称一些不相关的事情要求您开门。而您一旦开门，就会被实施逮捕。在这种情况下警方没有“闯入”，是您“主动”开门的。

所以，不要随便开门。

2019年5月22日，意大利的反法西斯活动家波巴在家中被逮捕，警方敲门时只是声称“需要口头警告”。警方还对他的住所进行了搜查，没收了电子设备。在这里看到该案件。

[image]
[image]

身体暴力(含酷刑)

身体暴力是指对手通过使用武力来威吓目标或其关系网、使目标失去行动能力，或迫使其透露信息。

身体暴力包括酷刑，且不限于。例如，在俄罗斯和白俄罗斯等国家，近年来有多名无政府主义者在被国家逮捕后遭到酷刑。这些国家报告的酷刑手段包括：殴打、用塑料袋或枕头窒息、往鼻孔和嘴里灌水、倒挂双腿或绑住双手、电击、用螺丝刀施刑、强迫做深蹲直到筋疲力尽倒下、性暴力，以及剥夺睡眠、食物和水。

在某些情况下，身体暴力也可能包括暗杀。

[image]

返回：[image]为最坏的情况做准备，迎接最好的结果如何在敌对环境中保护自己S02E04

□

延伸：https://web.archive.org/web/20250601034455/https://iyouport.substack.com/p/342

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

加密

加密的目的是尽可能让任何没有解密密钥（通常是密码）的人都无法解读数据。加密可以应用于“静态”数据（例如存储在计算机上的文件）和“动态”数据（例如消息应用程序中传递的消息）。

延伸：https://iyouport.substack.com/p/548?utm_source=publication-search

您可以通过在设备上启用全盘加密 (FDE) 并使用强密码来加密数字设备上的“静态”数据。设备关机时，其数据会被加密；开机并输入解密密钥后，其数据会被解密，直至关机。如果启用全盘加密的设备在关机状态下被对手在查抄（抄家 、 [image]隐蔽性地突袭住所 等），对手将无法访问其数据（除非他们能实现 身份验证绕过 ）。

您可以使用 Tor 加密“动态”数据，使用虚拟专用网络 (VPN) 进行所有互联网活动，使用端到端加密消息应用程序进行数字通信。加密“动态”数据可以防止对手监视您的数字活动。

加密应该被视为一种减少伤害的措施，而非万能药。除非不可避免，否则 不应 使用数字设备进行高度危险的活动，并且所有可能造成定罪的对话都应该 采取 **[image]** 户外无设备对话 原则 ，并且不要携带和使用电子设备 。

此自卫措施用于应对的镇压手段

[image]
[image]

移动网络运营商

移动网络运营商与当局合作提供有关您的私密信息，是很常见的状况。

它们可以提供：

- 给定一个姓名：找到该姓名注册过的所有电话号码。
- 给定一个电话号码：注册该电话号码的人的姓名和使用该电话号码的手机的IMEI号码。
- 给定一个IMEI号码：使用该IMEI号码的手机的电话号码。

此外，移动网络运营商还可以根据您的电话号码提供有关您手机活动的数据和元数据 —— 当前的和历史的。

- 所有短信内容和您用手机拨打的常规电话。
- 您用手机访问过的网站列表。
- 您的手机的物理位置（它被带着去过哪些地方）。
- 有关您使用端到端加密信息应用程序的元数据（例如，您何时使用 Signal 以及通过 Signal 发送或接收的信息的大致大小）。这就是为什么说元数据不加密是一个问题。

这意味着，以下任何一种情况都可能让对手在移动网络运营商的配合下，获取有关的您手机活动的（当前和历史）数据和元数据：

- 知道您的姓名（如果您的手机不是匿名的）。

- 知道您的手机号码，他们可以通过监控或扣押与您有联系的手机、使用 IMSI 捕获器（黄貂鱼）、或通过高级关联技术找到您的手机号码。例如，如果对手知道您周一在地点 A，周二在地点 B，并且他们从手机信号塔数据中得知某部手机是唯一一部周一在地点 A、周二在地点 B 的手机，那么他们就可以推断出这部手机是您的。即便手机号没有实名，追溯您的身份也不是难事。

- 知道您的手机IMEI号码，他们可以通过扣押您的手机找到您的IMEI号码。

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

[image]

返回：[image]买不起/买不到一次性手机怎么办？这里是您在参加敏感行动之前需要了解的事

对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

身份检查

身份核查是指国家通过要求个人提供个人信息、出示政府颁发的身份证件，或采集其生物识别信息（如面部照片、指纹、DNA）并与数据库进行比对，以验证个人身份的过程。身份核查可能成为盘问和施压的借口，并可能导致对个人随身物品的强行搜查。

配合身份核查会使国家获取您的个人信息，这有助于他们绘制您的社交网络，若你被通缉，还可能导致您更容易被逮捕。

无法配合或拒绝配合身份核查的后果高度依赖具体情境，但可能包括被强制采集生物特征信息（或在不知情的情况下被采集）、被拘留，以及被驱逐出境。

被身份检查针对的可能性取决于具体情况、以及您在国家机器眼中的形象。如果您从事不引人注目的活动、并且穿得看起来像个有钱人，被针对的可能性就较低。如果您被视为潜在犯罪分子或“非法移民”，或者在进入或离开起义现场时，被针对的可能性就会较高。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]

信息最小化原则

信息最小化作为一项安全原则，规定：敏感信息应仅在必要时共享，且仅在必要的范围内共享。该原则通过控制网络信息流，使其对外界更加不透明，更难被破坏，从而使镇压更加困难。

信息最小化也是防止渗透告密的有效措施之一。

应用信息最小化的行动属于最高级别的保密标准。您应该首先分析您的行动属于哪一种。可以在下面看到对安全分级的简要描述。

[image] 您可以点击右上角三个点 - “更多选项” - “查看原始内容”，以获得大图。或者直接下载到您本地查阅和保存。

对于一项行动，不论是计划中的还是很久前已经完成的，信息最小化原则要求：

- 没有亲自参与该行动的所有人，不应猜测谁参与其中。
- 参与行动的所有人，不应向未参与行动的任何人透露其参与的情况。
- 在行动中扮演特定且有限角色的人，可能不需要知道除了与自己直接沟通的人之外还有谁参与其中。

[image]

返回（关于角色分配和不同阶段的要求）：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

同时，每一位队友都有权及时阻止违反信息最小化原则的行为 —— 例如，如果您听到有人在谈论自己参与了某项行动，或者在猜测其他谁谁也参与其中了，请立即阻止这种对话。

在您自己的亲密团队内部严格要求保密分级可能不会太困难，只要大家具有强烈的战略共识，就能主动配合。但如果您的项目较大，需要多个团队和组织的联合才能实现，这种情况下就需要管理一下了 —— 一般来说需通过“发言人委员会”来协调信息最小化原则。

在这种结构中，每个团体指定一到两人参加发言人委员会，并与其他团体的指定人员会面。这样，各团体就可以通过发言人委员会进行协调，而无需其他任何人了解所有参与者。

不过要注意的是，这种结构存在造成协调“瓶颈”的风险 —— 如果某个人是两个团体之间唯一的桥梁，这就可能会造成一种守门人的特权状态，而且如果此人被对手逮捕了，协调也将变得不可能。

需要为这种情况留出**Plan B**。

详细步骤见下文。

[image]

返回：[image]安全文化：帮助最大程度上减轻被监视和被渗透的恐慌

返回：[image]安全文化和广阔的生活

推荐相关资料

- Secrets And Lies

此自卫措施用于应对的镇压手段

[image]

地形侦查

地形侦查是收集有关行动目标的信息。

侦查在制定周密的行动计划 之前进行。

侦察可以通过物理方式（例如前往计划中的行动现场进行观测）、或者使用数字方式（例如通过网络研究目标等等）。

请开启沉浸式。在侦察过程中，您应该像在实际行动中一样，充分考虑对手可能对您使用的所有 ☠镇压手段 。

更多具体步骤详见：

[image]

返回：[image]直接行动分步指南：它是什么、它有什么用、如何获得成功

[image]

物理侦查

物理侦察的例子包括：

- 检查往返行动现场的所有可能路线，评估哪些路线比较合适。例如，一条好的路线的标准包括：沿途上监控摄像头覆盖范围最小，并且有合适的地点可以在行动前和之后更换衣服。

- 检查行动现场及其周边，寻找所有固定的监控摄像头偷拍 系统、 [image]警卫、 报警系统 ，和攻击目标的机会。

进行物理侦察时，您可以：

- 执行[image]反监视 策略，以应对物理监视的风险。
- 采取[image]匿名着装 原则，以应对被观察或记录的风险。

数字侦察

数字侦察的例子包括：

- 数字开源情报调查https://start.me/w/bbk9Bo
- 在线地图上检查行动地点，及其周边。

强调：进行侦察时，您应该遵循数字安全最佳实践。

此自卫措施用于应对的镇压手段

[image]

元数据擦除和避免

元数据是关于数据的数据，即关于其他信息的信息。元数据擦除是指删除已有的元数据。元数据避免是指数字系统从一开始就不创建元数据，或者加密其创建的元数据使其无法被攻击者读取。

[image]

返回：[image]少即是多：变得难以被追踪的简单方法 S03E05

元数据示例

元数据包括：

- 图像文件可能嵌入了有关拍摄时间、地点以及拍摄设备的详细信息。

- PDF 文件可能嵌入了有关创建它的计算机的信息。

- 电子邮件中嵌入了收发双方的电子邮件地址。

- 打印的文档通常带有不可见的水印 —— 微点，标识打印该文档的打印机的品牌和型号。 延伸：https://iyouport.substack.com/p/-3-151 ；以及更多相关详细说明 https://dys2p.com/en/2022-09-print-scan-traces.html

元数据擦除

对于数字文件，有很多工具可用来擦除元数据，比如https://github.com/tpet/mat2 、或者https://gitlab.com/rmnvgr/metadata-cleaner/，再或者，请从本站“工具”专题中搜索“元数据”，以找到可能适合您的解决方案。

一些注重安全的操作系统默认包含元数据擦除工具。见 [image]数字技术限制和最佳实践

[image]

元数据避免

元数据避免的方法包括：

- 使用专用操作系统（例如 Tails）创建或修改数字文件，以便有关您通常使用的操作系统的信息不会嵌入到文件的元数据中。
- 使用可抗元数据的消息传递应用程序。 [image]数字技术限制和最佳实践

此自卫措施用于应对的镇压手段

[image]
🔥

纵火

纵火取证（也称为火灾调查）分为两个不同的阶段：火灾现场调查（侧重于火灾现场的证据）和火灾残骸分析（侧重于从现场提取残骸并在实验室进行分析的证据）。

火灾现场调查包括两大主题：确定火灾是否为人为纵火，以及识别其起火点。

当火灾达到“闪燃点”时，调查难度会大大增加 —— 即房间温度升高到足以使所有可燃表面瞬间起火的程度。

火灾残留物分析专注于可燃液体残留物（ILRs），旨在识别潜在的助燃剂痕迹及其化学成分 —— 这些样本通常是由警犬在现场发现的。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

匿名手机

匿名手机是指不与您的身份绑定的手机。一次性手机是指使用后不久就会丢弃的匿名手机。

[image]

[image]

返回：[image]一次性手机用户指南：关于刻录机电话您应该知道的重要原则

[image]

返回：[image]当您准备参加抗议活动：基本指南

返回：[image]在街上保持安全：街头实战指南 S05E12

Edward Snowden: "Both Apple and Android devices unfortunately are not especially good in protecting your privacy."Every phone, even when the screen is off you think it's doing nothing, but it's screaming 'Here I am'.""They can see everything about you. They can see everything about what your device is doing, and they can do whatever they want with your device.” attachment:d806f276-ef16-44bd-ad0c-bfef83fa70f0:cXRgqikhBzdSUR_F.mp4

匿名手机

对于敏感行动和聚会，您首先应该衡量是否真的需要携带手机。因为行动团队中有不同的角色，同时也有不同的计划，所以需求肯定不

同。以风险最小化为原则，基于您的需求进行具体的部署。

如果您确定需要使用手机，可以使用匿名手机。除非需要长期保持电话号码稳定，否则最好使用一次性的手机。

设置和使用匿名手机的要点：

- 匿名购买 手机、SIM 卡和套餐。
- 永远不要在您的真实住所（和工作单位/学校）附近开机，因为对手可以通过与移动网络运营商的合作了解手机物理位置的历史记录。 返回威胁矩阵查看相关内容 [image]移动网络运营商

“假匿名”电话

假匿名手机是指您 匿名购买 的但是在居住地附近使用的手机。它们可以缓解 网络映射 —— 尤其是在场景或关系网络中所有成员都使用这种手机的情况下 —— 但是您不应将“假匿名”手机用于敏感项目或行动。

[image]

返回：[image]手机应该有且只有一个用途：如何在敌对环境中保护自己 S02E03

返回；[image]如果您的手机被盗或被警察抢走…

此自卫措施用于应对的镇压手段

[image]
👎

栽赃

制造虚假证据或篡改真实证据，以达到指控目标人的目的。

典型的栽赃手段包括：

- 在警方报告中撒谎。
- 栽赃证据。例如，美国巴尔的摩的警察并不知道他们佩戴的身体摄像头在手动“关闭”后仍在继续录制，结果录下了他们将毒品塞进嫌疑人包里的过程。

根据具体情况，证据造假可能较为常见，也可能较为罕见。总之，要警惕这种手段。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]
[image]

隐蔽的监视设备

对手隐藏了电子设备，用于收集数据：音频、视频和位置数据。

[image]

返回：[image]您是否正在被 AirTag 跟踪？这里是检查方法

隐藏的监视设备一般会出现在哪儿

对手可以在建筑物内、或车子内外，以及户外隐藏秘密监视设备。

值得注意的地点包括：

- 隐藏在目标住所内的窃听器和摄像头。
- 隐藏在目标车辆内外的定位追踪器。
- 隐藏在目标住宅附近建筑物窗户处的监视摄像头，以便摄像头能够拍摄住宅的入口，或特定房间窗口。

隐藏的监视设备可能存在多久

对手可以隐藏秘密监视设备进行长期的监视（例如数周、数月甚至数年），或者针对特定事件进行短期的监视。

秘密监视设备可能在这些情况下被移除：

- 最常见的情况是安装者亲自将其取回。
- 在某些情况下，被第三方意外发现，将其移除。
- 在极少数情况下，经当事人或第三方主动检测而发现，并移除。

电力

隐蔽的监控设备需要电源供应，可以是电池，也可以是设备所在之处的建筑物内或车辆内的电气系统，或者两者兼有。在极少数情况下，它们还可能使用以太网供电（PoE）。为了节省电池电量并使其更难被发现，设备可能不会一直处于通电状态。

数据传输

隐蔽的监控设备通常会传输它们收集的数据：

- 对于低成本的现代设备，通常通过设备内置的SIM卡经移动通信网络传输。
- 部分设备可通过Wi-Fi、蓝牙、以太网或任意射频传输。

部分设备从不传输所收集的数据：攻击者需物理接触设备才能获取数据。

📌 对应的镇压战术：指控。

3个子项目

[image]

弹道学

弹道取证是将科学应用于枪支和子弹的调查。子弹射出时，枪会在子弹和弹壳上留下微小的痕迹。这些痕迹就像弹道指纹一样。

当对手回收一颗子弹时，法医鉴定人员可以对嫌疑人的枪支进行试射，然后将回收子弹上的痕迹与试射子弹上的痕迹进行比较。弹壳的比较方式相同。

对应的镇压战术：指控。

自卫措施

[image]

抄家

抄家是指对手对住宅进行突击搜查，以扣押物品、逮捕住户、或强行安装监控设备。

通常什么时候发生

抄家经常发生在：

- 通常在清晨，天亮之前，屋内的人正在熟睡，最猝不及防的时候。

- 在某些情况下，抄家会在白天进行。例如，当突袭的目的之一是查获正在运行的数字设备的时候 —— 此时其加密功能可能无效。这种情况下对手可能选择在白天进行突袭，因为数字设备在用户清醒的情况下更可能处于运行状态。

抄家的目的

对手实施抄家的目的可能包括：

- 扣押物品以寻找证据或进行网络映射（连锅端）。常见的扣押物品包括电子设备、文献、可用于行动的材料以及衣物。在某些情况下，对手会扣押昂贵物品（如电脑、打印设备），以破坏目标组织的运作能力。

- 逮捕住宅内的居民。
- 在住宅内安装监控设备。

其他考虑因素

在某些国家，当国家机器进行突袭时，仅允许搜查搜查令中列名的房间。如果您和您的组织有面临此类风险的可能性，请参考本地法律，记住您的权利。

📌 对应的镇压战术：指控、逮捕。

自卫措施

镇压行动案例

[image]
🚁

空中监视

空中物理监视是指从空中直接观察人员或活动以收集信息。在许多国家，直升机传统上是进行此类监视的主要工具。随着无人机成本的降低，其使用正变得越来越普遍。侦查机也偶尔被使用，且比直升机隐蔽得多。采取哪种工具，取决于监视目标的地形、范围、组成。

延伸：https://iyouport.substack.com/p/lr--bc3?utm_source=publication-search

延伸：https://iyouport.substack.com/p/0c8?utm_source=publication-search

延伸：https://iyouport.substack.com/p/isis?utm_source=publication-search

[image]

返回：[image]空中监视如何追踪抗议者？

返回：[image]5种常用的“击落”无人机的方法

空中物理监视的示例包括：

- 在示威或集会期间监视人群，通常作为公开监视行动的一部分。

- 在秘密监视行动中提高成功跟踪监视目标的几率，尤其是在夜间。

- 在行动发生后迅速定位嫌疑人，尤其是在农村地区或在夜间（例如德国的一起纵火案中，警方直升机当晚就飞越了该地区）。 案件详情：https://actforfree.noblogs.org/post/2023/11/13/munich-germany-geothermal-energy-gets-hot-and-not-only

- 在激进活动高发区域进行常规警察巡逻时定位嫌疑人。

- 监视飞机可监控整个城市，每秒拍摄多达**80**平方公里， 实现对几乎任何户外活动的慢动作重建 ，并具有很好的夜视功能 在夜间也能提供高质量视频 。

📌 对应的镇压战术：指控。

自卫措施

镇压行动案例

[image]

监视器排查

是指主动排查可能隐藏的监视设备。特定的建筑物内外、车内、住宅内外等。

一种是手动目视搜索，另一种是采用专门的设备。比如手机查找隐藏的摄像头，等等。

[image]

返回：[image]物理入侵检测 - 查找隐藏的摄像头和防入侵：把移动设备变成监测仪

排查的目的

全面有效地排查所有可能存在的监视器需要极高的技术专长。如果您缺乏这方面的专业知识，在搜索某个区域内的监视器时，您可能无法确定是否找到了该区域内的所有隐藏的设备。

因此，这里所说的“排查”的目的应该是防止对手收集您的信息，而不是旨在找到一切隐蔽的监控装置。换句话说，您应该有这样的意识：任何可能被用来指控您和队友的对话和行为都应该始终选择在户外进行，且确认周围没有公共监视器，尤其是参与对话的所有人不该携带电子设备。

[image]

返回：[image]户外无设备对话

手动目视搜索

这是主要的常规做法。

- 如果排查目标是一栋建筑，可以使用合适的工具拆卸电源插座、接线板、天花板灯以及任何电器，寻找不该出现的东西。也可以检查家具内部，床下等。

- 如果排查目标是车辆，可以查看车底、车轮内侧、后保险杠、通风口后方等处，寻找任何不该出现的东西。也可以使用合适的工具拆卸内饰、车顶、仪表板、头枕等等。对于摩托车或自行车，可以查看座椅内或下方。与其他车辆不同，搜查自行车时可以有把握地确定是否存在窃听器。所以敏感的行动或逃脱过程中更推荐使用无标记的自行车 BACK [image]自行车接力

- 如果您正在搜寻街上的监控车辆中安装的摄像头，可采用被动 [image]监控侦测 方法。

专业检测设备

第二种方法是使用专门的检测设备。这类设备可以在专卖店或网上购买，包括：

- 射频探测器，用于检测搜索时正在通过射频传输数据的设备。

- 针孔相机镜头检测器，用来搜索可能隐藏的摄像头。

- 专业设备 —— 频谱分析仪、非线性节点探测器、热成像系统 —— 可能更有效，但使用起来非常昂贵且复杂。 除非您确实有条件且认为必要，否则不推荐。

□

延伸：这里是一个专门针对无政府主义者和其他激进反叛前线工作者进行镇压的秘密监视设备数据库，您可以来大致感受一下这种手段有多可怕： https://www.notrace.how/earsandeyes/#

此自卫措施用于应对的镇压手段

[image]

道路封锁

道路封锁是为了控制或阻断特定道路的交通而设置的临时设施。

镇压者设置道路封锁，是为了：

- 作为一项有计划的措施，例如在已知将要发生抗议活动的街道周围，控制抗议者的流量。
- 临时围堵，例如在某项行动之后镇压者想要抓住参与该行动的人。

在某些情况下，警方会在某些事件发生后系统地设置路障，例如引人注目的抢劫案或越狱事件。

自卫措施

镇压行动案例

[image]

平民告密

是指不属于敌方侦查人员的随机平民，向敌方举报您。比如“自干五”、法西斯分子等等；或者因遭到警方问讯而提供了关于您的任何信息的“目击者”。

📌 对应的镇压战术：威慑、指控。

自卫措施

镇压行动案例

[image]

刑侦证据洗白

即所谓的平行构建。指的是执法部门在调查过程中非法建立平行或独立的证据基础，以掩盖调查的实际进行方式。

例如，情报机构可以在没有搜查令的情况下从目标人的手机中收集有罪证据，然后再进行搜查行动没收那部手机，以便在法庭上假装“发现”这些证据，从而避免因非法获取而被排除。

平行构建的一种特殊形式是证据洗白，即一名警察非法收集的证据，然后转交给其他人进行“洗白”—— 通过将证据转交另一名警察进行演变，再由该警察移交检察官。

比如，美国的第四修正案规定不得进行不合理的搜查和扣押。如果一名警察A获取证据的手段正是来自于“不合理的搜查和扣押”，那么这个证据就无法直接使用了，法庭会因其违宪而拒绝。这种情况下，这个证据会被转交给另外一名警察B，利用该警察“诚信例外”适用性，使法院接受该证据。

延伸：https://www.hrw.org/news/2018/01/09/us-secret-evidence-erodes-fair-trial-rights

延伸：https://www.theregister.co.uk/2016/12/06/parallel_construction_lies_in_english_courts/

延伸：https://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/

📌 对应的镇压战术：指控。